# 3Com Switch 4500G Family

## Configuration Guide

Switch 4500G 24-Port

Switch 4500G 48-Port

Switch 4500G PWR 24-Port

Switch 4500G PWR 48-Port

Product Version:
V05.02.00
Manual Version:
6W100-20090210
www.3com.com

**3Com Corporation**
350 Campus Drive, Marlborough,
MA, USA 01752 3064

## ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

### End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

### Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

### Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# About This Manual

## Organization

*3Com Switch 4500G Family Configuration Guide* is organized as follows:

| Volume | Features | | | |
|---|---|---|---|---|
| 00-Product Overview | Product Overview | Acronyms | | |
| 01-Access Volume | Ethernet Interface | Link Aggregation | Port Isolation | DLDP |
| | LLDP | MSTP | Smart Link | Monitor Link |
| | VLAN | GVRP | QinQ | BPDU Tunneling |
| | Ethernet OAM | Connectivity Fault Detection | RRPP | Port Mirroring |
| 02-IP Services Volume | IP Addressing | ARP | DHCP | DNS |
| | IP Performance Optimization | UDP Helper | IPv6 Basics | Dual Stack |
| | sFlow | | | |
| 03-IP Routing Volume | IP Routing Overview | Static Routing | RIP | IPv6 Static Routing |
| | RIPng | Route Policy | | |
| 04-Multicast Volume | Mulitcast Overview | IGMP Snooping | Multicast VLAN | MLD Snooping |
| | IPv6 Multicast VLAN | | | |
| 05-QoS Volume | QoS | User Profile | | |
| 06-Security Volume | AAA | 802.1X | HABP | MAC Authentication |
| | Portal | Port Security | IP Source Guard | SSH2.0 |
| | PKI | SSL | Public Key | ACL |
| 07-System Volume | Login | Basic System Configuration | Device Management | File System Management |
| | HTTP | SNMP | RMON | MAC Address Table Management |
| | System Maintaining and Debugging | Information Center | PoE | Track |
| | NQA | NTP | Hotfix | Cluster Management |
| | Stack Management | Automatic Configuration | | |

# Conventions

The manual uses the following conventions:

## Command conventions

| Convention | Description |
|---|---|
| **Boldface** | The keywords of a command line are in **Boldface**. |
| *italic* | Command arguments are in *italic*. |
| [ ] | Items (keywords or arguments) in square brackets [ ] are optional. |
| { x \| y \| ... } | Alternative items are grouped in braces and separated by vertical bars. One is selected. |
| [ x \| y \| ... ] | Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected. |
| { x \| y \| ... } * | Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected. |
| [ x \| y \| ... ] * | Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected. |
| &<1-n> | The argument(s) before the ampersand (&) sign can be entered 1 to n times. |
| # | A line starting with the # sign is comments. |

## GUI conventions

| Convention | Description |
|---|---|
| < > | Button names are inside angle brackets. For example, click <OK>. |
| [ ] | Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window. |
| / | Multi-level menus are separated by forward slashes. For example, [File/Create/Folder]. |

## Symbols

| Convention | Description |
|---|---|
|  **Warning** | Means reader be extremely careful. Improper operation may cause bodily injury. |
|  **Caution** | Means reader be careful. Improper operation may cause data loss or damage to equipment. |
|  **Note** | Means a complementary description. |

## Related Documentation

In addition to this manual, each 3com Switch 4500G documentation set includes the following:

| Manual | Description |
| --- | --- |
| 3Com Switch 4500G Family Command Reference Guide | Provide detailed descriptions of command line interface (CLI) commands, that you require to manage your switch. |
| 3Com Switch 4500G Family Getting Started Guide | This guide provides all the information you need to install and use the 3Com Switch 4500G Family. |

## Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

# Table of Contents

# 1 Product Features

## Introduction to Product

3Com Switches 4500G are Gigabit Ethernet switching products which have abundant service features. They are designed as distribution and access devices for intranets and metropolitan area networks (MANs). They can also be used for connecting server groups in data centers.

## Feature Lists

3Com Switches 4500G support abundant features and the related documents are divided into the volumes as listed in Table 1-1.

**Table 1-1** Feature list

| Volume | Features | | | |
|---|---|---|---|---|
| 01-Access Volume | Ethernet Interface | Link Aggregation | Port Isolation | DLDP |
| | LLDP | MSTP | Smart Link | Monitor Link |
| | VLAN | GVRP | QinQ | BPDU Tunneling |
| | Ethernet OAM | Connectivity Fault Detection | RRPP | Port Mirroring |
| 02-IP Services Volume | IP Addressing | ARP | DHCP | DNS |
| | IP Performance Optimization | UDP Helper | IPv6 Basics | Dual Stack |
| | sFlow | | | |
| 03-IP Routing Volume | IP Routing Overview | Static Routing | RIP | IPv6 Static Routing |
| | RIPng | Route Policy | | |
| 04-Multicast Volume | Mulitcast Overview | IGMP Snooping | Multicast VLAN | MLD Snooping |
| | IPv6 Multicast VLAN | | | |
| 05-QoS Volume | QoS | User Profile | | |
| 06-Security Volume | AAA | 802.1X | HABP | MAC Authentication |
| | Portal | Port Security | IP Source Guard | SSH2.0 |
| | PKI | SSL | Public Key | ACL |

| Volume | Features | | | |
|---|---|---|---|---|
| 07-System Volume | Login | Basic System Configuration | Device Management | File System Management |
| | HTTP | SNMP | RMON | MAC Address Table Management |
| | System Maintaining and Debugging | Information Center | PoE | Track |
| | NQA | NTP | Hotfix | Cluster Management |
| | Stack Management | Automatic Configuration | | |

# 2 Features

The following sections provide an overview of the main features of each module supported by the 3Com Switch 4500G.

## Access Volume

**Table 2-1** Features in Access volume

| Features | Description |
|---|---|
| Ethernet Interface | This document describes:<br>• Combo Port Configuration<br>• Basic Ethernet Interface Configuration<br>• Configuring Flow Control on an Ethernet Interface<br>• Configuring the Suppression Time of Physical-Link-State Change on an Ethernet Interface<br>• Configuring Loopback Testing on an Ethernet Interface<br>• Configuring a Port Group<br>• Configuring Storm Suppression<br>• Setting the Interval for Collecting Ethernet Interface Statistics<br>• Enabling Forwarding of Jumbo Frames<br>• Enabling Loopback Detection on an Ethernet Interface<br>• Configuring the MDI Mode for an Ethernet Interface<br>• Testing the Cable on an Ethernet Interface<br>• Configuring the Storm Constrain Function on an Ethernet Interface |
| Link Aggregation | Link aggregation aggregates multiple physical Ethernet ports into one logical link. This document describes:<br>• Basic Concepts of Link Aggregation<br>• Configuring an Aggregation Group<br>• Configuring an Aggregate Interface<br>• Configuring a Load Sharing Mode for Load-Sharing Link Aggregation Groups |
| Port Isolation | The port isolation feature allows you to isolate different ports within the same VLAN. This document describes:<br>• Introduction to Port Isolation<br>• Configuring the Isolation Group |
| DLDP | In the use of fibers, link errors, namely unidirectional links, are likely to occur. DLDP is designed to detect such errors. This document describes:<br>• DLDP Introduction<br>• Enabling DLDP<br>• Setting DLDP Mode<br>• Setting the Interval for Sending Advertisement Packets<br>• Setting the DelayDown Timer<br>• Setting the Port Shutdown Mode<br>• Configuring DLDP Authentication<br>• Resetting DLDP State |

| Features | Description |
| --- | --- |
| LLDP | LLDP enables a device to maintain and manage its own and its immediate neighbor's device information, based on which the network management system detects and determines the conditions of the communications links. This document describes:<br>• Introduction to LLDP<br>• Performing Basic LLDP Configuration<br>• Configuring the Encapsulation Format for LLDPDUs<br>• Configuring the Encapsulation Format of the Management Address<br>• Configuring CDP Compatibility<br>• Configuring LLDP Trapping |
| MSTP | MSTP is used to eliminate loops in a LAN. It is compatible with STP and RSTP. This document describes:<br>• Introduction to MSTP<br>• Configuring the Root Bridge<br>• Configuring Leaf Nodes<br>• Performing mCheck<br>• Configuring Digest Snooping<br>• Configuring No Agreement Check<br>• Configuring Protection Functions |
| Smart Link | Smart Link is a solution for active-standby link redundancy backup and rapid transition in dual-uplink networking. This document describes:<br>• Smart Link Overview<br>• Configuring a Smart Link Device<br>• Configuring an Associated Device |
| Monitor Link | Monitor link is a port collaboration function used to enable a device to be aware of the up/down state change of the ports on an indirectly connected link. This document describes:<br>• Monitor Link Overview<br>• Configuring Monitor Link |
| VLAN | Using the VLAN technology, you can partition a LAN into multiple logical LANs. This document describes:<br>• Introduction to VLAN<br>• Types of VLAN<br>• Introduction and Configuration of Isolate-user-vlan<br>• Introduction and Configuration of Voice VLAN |
| GVRP | GVRP is a GARP application. This document describes:<br>• GARP overview<br>• GVRP configuration<br>• GARP Timers configuration |
| QinQ | As defined in IEEE802.1Q, 12 bits are used to identify a VLAN ID, so a device can support a maximum of 4094 VLANs. The QinQ feature extends the VLAN space by allowing Ethernet frames to travel across the service provider network with double VLAN tags. This document describes:<br>• Introduction to QinQ<br>• Configuring basic QinQ<br>• Configuring Selective QinQ<br>• Configuring the TPID Value in VLAN Tags |

| Features | Description |
| --- | --- |
| BPDU Tunneling | BPDU tunneling enables transparently transmission of customer network BPDU frames over the service provider network. This document describes:<br>• Introduction to BPDU Tunneling<br>• Configuring BPDU Transparent Transmission<br>• Configuring Destination Multicast MAC Address for BPDU Tunnel Frames |
| Ethernet OAM | Ethernet OAM is a tool monitoring Layer-2 link status. It helps network administrators manage their networks effectively. This document describes:<br>• Ethernet OAM overview<br>• Configuring Basic Ethernet OAM Functions<br>• Configuring Link Monitoring<br>• Enabling OAM Loopback Testing |
| Connectivity Fault Detection | Connectivity fault detection is an end-to-end, per-VLAN link-layer OAM mechanism for link connectivity detection, fault verification, and fault location. This document describes:<br>• Connectivity Fault Detection Overview<br>• Basic Configuration Tasks<br>• Configuring CC on MEPs<br>• Configuring LB on MEPs<br>• Configuring LT on MEPs |
| RRPP | RRPP is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes after a link is disconnected on the ring. This document describes:<br>• RRPP overview<br>• Configuring Master Node<br>• Configuring Transit Node<br>• Configuring Edge Node<br>• Configuring Assistant Edge Node<br>• Configuring Ring Group |
| Port Mirroring | Port mirroring copies packets passing through a port to another port connected with a monitoring device for packet analysis to help implement network monitoring and troubleshooting. This document describes:<br>• Port Mirroring overview<br>• Local port mirroring configuration<br>• Remote port mirroring configuration |

# IP Services Volume

**Table 2-2** Features in the IP Services volume

| Features | Description |
|---|---|
| IP Address | An IP address is a 32-bit address allocated to a network interface on a device that is attached to the Internet. This document describes:<br>• Introduction to IP addresses<br>• IP address configuration |
| ARP | Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address. This document describes:<br>• ARP Overview<br>• Configuring ARP<br>• Configuring Gratuitous ARP<br>• Proxy ARP and Local Proxy ARP configuration<br>• ARP Attack Defense configuration |
| DHCP | DHCP is built on a client-server model, in which the client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client. This document describes:<br>• DHCP relay agent configuration<br>• DHCP Client configuration<br>• DHCP Snooping configuration<br>• BOOTP Client configuration |
| DNS | Used in the TCP/IP application, Domain Name System (DNS) is a distributed database which provides the translation between domain name and the IP address. This document describes:<br>• Configuring the DNS Client<br>• Configuring the DNS Proxy |
| IP Performance | In some network environments, you need to adjust the IP parameters to achieve best network performance. This document describes:<br>• Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network<br>• Configuring TCP Attributes<br>• Configuring ICMP to Send Error Packets |
| UDP Helper | UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified server. This document describes:<br>• UDP Helper overview<br>• UDP Helper configuration |
| IPv6 Basics | Internet protocol version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet protocol version 4 (IPv4). This document describes:<br>• IPv6 overview<br>• Basic IPv6 functions configuration<br>• IPv6 NDP configuration<br>• PMTU discovery configuration<br>• IPv6 TCP properties configuration<br>• ICMPv6 packet sending configuration<br>• IPv6 DNS Client configuration |

| Features | Description |
|---|---|
| Dual Stack | A network node that supports both IPv4 and IPv6 is called a dual stack node. A dual stack node configured with an IPv4 address and an IPv6 address can have both IPv4 and IPv6 packets transmitted. This document describes:<br>• Dual stack overview<br>• Dual stack configuration |
| sFlow | Based on packet sampling, Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics. This document describes:<br>• sFlow Overview<br>• sFlow Configuration |

# IP Routing Volume

**Table 2-3** Features in the IP Routing volume

| Features | Description |
|---|---|
| IP Routing Overview | This document describes:<br>• Introduction to IP routing and routing table<br>• Routing protocol overview |
| Static Routing | A static route is manually configured by the administrator. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications. This document describes:<br>• Static route configuration<br>• Detecting Reachability of the Static Route's Nexthop |
| RIP | Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks. This document describes:<br>• RIP basic functions configuration<br>• RIP advanced functions configuration<br>• RIP network optimization configuration |
| IPv6 Static Routing | Static routes are special routes that are manually configured by network administrators. Similar to IPv4 static routes, IPv6 static routes work well in simple IPv6 network environments. This document describes:<br>• IPv6 static route configuration |
| IPv6 RIPng | RIP next generation (RIPng) is an extension of RIP-2 for IPv4. RIPng for IPv6 is IPv6 RIPng. This document describes:<br>• Configuring RIPng Basic Functions<br>• Configuring RIPng Route Control<br>• Tuning and Optimizing the RIPng Network |
| Routing Policy | Routing policy is used on the router for route inspection, filtering, attributes modifying when routes are received, advertised, or redistributed. This document describes:<br>• Defining Filters<br>• Route policy configuration |

# Multicast Volume

**Table 2-4** Features in Multicast volume

| Features | Description |
|---|---|
| Multicast Overview | This document describes the main concepts in multicast:<br>• Introduction to Multicast<br>• Multicast Models<br>• Multicast Architecture<br>• Multicast Packets Forwarding Mechanism |
| IGMP Snooping | Running at the data link layer, IGMP Snooping is a multicast control mechanism on the Layer 2 Ethernet switch and it is used for multicast group management and control. This document describes:<br>• Configuring Basic Functions of IGMP Snooping<br>• Configuring IGMP Snooping Port Functions<br>• Configuring IGMP Snooping Querier<br>• Configuring IGMP Snooping Policy |
| Multicast VLAN | Multicast VLAN configuration |
| MLD Snooping | Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. This document describes:<br>• Configuring Basic Functions of MLD Snooping<br>• Configuring MLD Snooping Port Functions<br>• Configuring MLD Snooping Querier<br>• Configuring MLD Snooping Policy |
| IPv6 Multicast VLAN | IPv6 Multicast VLAN configuration |

# QoS Volume

**Table 2-5** Features in the QoS ACL volume

| Features | Description |
|---|---|
| QoS | This document describes:<br>• QoS overview<br>• Traffic classification configuration<br>• Traffic policing Configuration<br>• Line rate configuration<br>• QoS policy configuration<br>• Congestion management<br>• Priority mapping configuration<br>• Traffic mirroring configuration |
| User Profile | User profile provides a configuration template to save predefined configurations. This document describes:<br>• Creating a User Profile<br>• Configuring a User Profile<br>• Enabling a User Profile |

# Security Volume

**Table 2-6** Features in the Security volume

| Features | Description |
|---|---|
| AAA | Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management. This document describes:<br>• Introduction to AAA, RADIUS and HWTACACS<br>• AAA configuration<br>• RADIUS configuration<br>• HWTACACS configuration |
| 802.1X | IEEE 802.1X (hereinafter simplified as 802.1X) is a port-based network access control protocol that is used as the standard for LAN user access authentication. This document describes:<br>• 802.1X overview<br>• 802.1X configuration<br>• 802.1X Guest-VLAN configuration |
| HABP | On an HABP-capable switch, HABP packets can bypass 802.1X authentication and MAC authentication, allowing communication among switches in a cluster. This document describes:<br>• Introduction to HABP<br>• HABP configuration |
| MAC Authentication | MAC authentication provides a way for authenticating users based on ports and MAC addresses; it requires no client software to be installed on the hosts. This document describes:<br>• RADIUS-Based MAC Authentication<br>• Local MAC Authentication |
| Portal | Portal authentication, as its name implies, helps control access to the Internet. This document describes:<br>• Portal overview<br>• Portal configuration |
| Port Security | Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1X authentication and MAC authentication. This document describes:<br>• Enabling Port Security<br>• Setting the Maximum Number of Secure MAC Addresses<br>• Setting the Port Security Mode<br>• Configuring Port Security Features<br>• Configuring Secure MAC Addresses<br>• Ignoring Authorization Information from the Server |
| IP Source Guard | By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. This document describes:<br>• Configuring a Static Binding Entry<br>• Configuring Dynamic Binding Function |

| Features | Description |
|---|---|
| SSH2.0 | SSH ensures secure login to a remote device in a non-secure network environment. By encryption and strong authentication, it protects the device against attacks. This document describes:<br>• Configuring Asymmetric Keys<br>• Configuring the Device as an SSH Server<br>• Configuring the Device as an SSH Client<br>• Configuring an SFTP Server<br>• Configuring an SFTP Client |
| PKI | The Public Key Infrastructure (PKI) is a hierarchical framework designed for providing information security through public key technologies and digital certificates and verifying the identities of the digital certificate owners. This document describes PKI related configuration. |
| SSL | Secure Sockets Layer (SSL) is a security protocol providing secure connection service for TCP-based application layer protocols, this document describes SSL related configuration. |
| Public Key Configuration | This document describes Public Key Configuration. |
| ACL | An ACL is used for identifying traffic based on a series of preset matching criteria. This document describes:<br>• ACL overview and ACL types<br>• ACL configuration |

# System Volume

**Table 2-7** Features in the System volume

| Features | Description |
|---|---|
| Login | Upon logging into a device, you can configure user interface properties and manage the system conveniently. This document describes:<br>• How to log in to your Ethernet switch<br>• Introduction to the user interface and common configurations<br>• Logging In Through the Console Port<br>• Logging In Through Telnet<br>• Logging in Through Web-based Network Management System<br>• Logging In Through NMS<br>• Specifying Source IP address/Interface for Telnet Packets<br>• Controlling Login Users |
| Basic System Configuration | Basic system configuration involves the configuration of device name, system clock, welcome message, user privilege levels and so on. This document describes:<br>• Configuration display<br>• Basic configurations<br>• CLI features |

| Features | Description |
| --- | --- |
| Device Management | Through the device management function, you can view the current condition of your device and configure running parameters. This document describes:<br>• Device management overview<br>• Rebooting a device<br>• Configuring the scheduled automatic execution function<br>• Specifying a file for the next device boot<br>• Upgrading Boot ROM<br>• Configuring a detection interval<br>• Configuring temperature alarm thresholds for a board<br>• Clearing the 16-bit interface indexes not used in the current system<br>• Configuring the system load sharing function<br>• Configuring the traffic forwarding mode of SRPUs<br>• Configuring the working mode of EA LPUs<br>• Enabling the port down function globally<br>• Enabling expansion memory data recovery function on a board<br>• Identifying and diagnosing pluggable transceivers |
| File System Management | A major function of the file system is to manage storage devices, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file. This document describes:<br>• File system management<br>• Configuration File Management<br>• FTP configuration<br>• TFTP configuration |
| HTTP | Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. This document describes:<br>• HTTP Configuration<br>• HTTPS Configuration |
| SNMP | Simple network management protocol (SNMP) offers a framework to monitor network devices through TCP/IP protocol suite. This document describes:<br>• SNMP overview<br>• Basic SNMP function configuration<br>• SNMP log configuration<br>• Trap configuration<br>• MIB style configuration |
| RMON | RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. This document describes:<br>• RMON overview<br>• RMON configuration |
| MAC Address Table Management | A switch maintains a MAC address table for fast forwarding packets. This document describes:<br>• MAC address table overview<br>• Configuring MAC Address Entries<br>• Configuring the Aging Timer for Dynamic MAC Address Entries<br>• Configuring the MAC Learning Limit<br>• Configuring MAC Information |

| Features | Description |
| --- | --- |
| System Maintenance and Debugging | For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors. This document describes:<br>• Maintenance and debugging overview<br>• Maintenance and debugging configuration |
| Information Center | As the system information hub, Information Center classifies and manages all types of system information. This document describes:<br>• Information Center Overview<br>• Setting to Output System Information to the Console<br>• Setting to Output System Information to a Monitor Terminal<br>• Setting to Output System Information to a Log Host<br>• Setting to Output System Information to the Trap Buffer<br>• Setting to Output System Information to the Log Buffer<br>• Setting to Output System Information to the SNMP Module<br>• Configuring Synchronous Information Output<br>• Disabling a Port from Generating Link Up/Down Logging Information |
| PoE | The Power over Ethernet (PoE) feature enables the power sourcing equipment (PSE) to feed powered devices (PDs) from Ethernet ports through twisted pair cables. This document describes:<br>• PoE overview<br>• Configuring the PoE Interface<br>• Configuring PoE power management<br>• Configuring the PoE monitoring function<br>• Online upgrading the PSE processing software<br>• Configuring a PD Disconnection Detection Mode<br>• Enabling the PSE to detect nonstandard PDs |
| Track | The track module is used to implement collaboration between different modules through established collaboration objects. The detection modules trigger the application modules to perform certain operations through the track module. This document describes:<br>• Track Overview<br>• Configuring Collaboration Between the Track Module and the Detection Modules<br>• Configuring Collaboration Between the Track Module and the Application Modules |
| NQA | NQA analyzes network performance, services and service quality by sending test packets to provide you with network performance and service quality parameters. This document describes:<br>• NQA Overview<br>• Configuring the NQA Server<br>• Enabling the NQA Client<br>• Creating an NQA Test Group<br>• Configuring an NQA Test Group<br>• Configuring the Collaboration Function<br>• Configuring Trap Delivery<br>• Configuring the NQA Statistics Function<br>• Configuring Optional Parameters Common to an NQA Test Group<br>• Scheduling an NQA Test Group |

| Features | Description |
| --- | --- |
| NTP | Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network. This document describes:<br>• NTP overview<br>• Configuring the Operation Modes of NTP<br>• Configuring Optional Parameters of NTP<br>• Configuring Access-Control Rights<br>• Configuring NTP Authentication |
| Hotfix | Hotfix is a fast, cost-effective method to fix software defects of the device without interrupting the running services. This document describes:<br>• Hotfix Overview<br>• One-Step Patch Installation<br>• Step-by-Step Patch Installation<br>• Step-by-Step Patch Uninstallation<br>• One-Step Patch Uninstallation |
| Cluster Management | A cluster is a group of network devices. Cluster management is to implement management of large numbers of distributed network devices. This document describes:<br>• Cluster Management Overview<br>• Configuring the Management Device<br>• Configuring the Member Devices<br>• Configuring Access Between the Management Device and Its Member Devices<br>• Adding a Candidate Device to a Cluster<br>• Configuring Advanced Cluster Functions |
| Stack Management | A stack is a set of network devices. Administrators can group multiple network devices into a stack and manage them as a whole. Therefore, stack management can help reduce customer investments and simplify network management. This document describes:<br>• Stack Configuration Overview<br>• Configuring the Master Device of a Stack<br>• Configuring Stack Ports of a Slave Device<br>• Logging In to the CLI of a Slave from the Master |
| Automatic Configuration | Automatic configuration enables a device to automatically obtain and execute the configuration file when it starts up without loading the configuration file. This document describes:<br>• Introduction to Automatic Configuration<br>• Typical Networking of Automatic Configuration<br>• How Automatic Configuration Works |

# Appendix A Acronyms

#ABCDEFGHIKLMNOPQRSTUVWXZ

| Acronyms | Full spelling |
|---|---|
| # | Return |
| 10GE | Ten-GigabitEthernet |
| **A** | Return |
| AAA | Authentication, Authorization and Accounting |
| ABC | Activity Based Costing |
| ABR | Area Border Router |
| AC | Alternating Current |
| ACK | ACKnowledgement |
| ACL | Access Control List |
| ADSL | Asymmetric Digital Subscriber Line |
| AFI | Address Family Identifier |
| ALG | Application Layer Gateway |
| AM | accounting management |
| ANSI | American National Standard Institute |
| AP | Access Point |
| ARP | Address Resolution Protocol |
| AS | Autonomous System |
| ASBR | Autonomous System Border Router |
| ASCII | American Standard Code for Information Interchange |
| ASE | Application service element |
| ASIC | Application Specific Integrated Circuit |
| ASM | Any-Source Multicast |
| ASN | Auxiliary Signal Network |
| AT | Advanced Technology |
| AT | Adjacency Table |
| ATM | Asynchronous Transfer Mode |
| AUX | Auxiliary (port) |
| **B** | Return |
| BC | Bearer Control |
| BDR | Backup Designated Router |
| BFD | Bidirectional Forwarding Detection |

| Acronyms | Full spelling |
|---|---|
| BGP | Border Gateway Protocol |
| BIMS | Branch Intelligent Management System |
| BOOTP | Bootstrap Protocol |
| BPDU | Bridge Protocol Data Unit |
| BRI | Basic Rate Interface |
| BSR | Bootstrap Router |
| BT | BitTorrent |
| BT | Burst Tolerance |
| **C** | Return |
| CA | Call Appearance |
| CA | Certificate Authority |
| CAR | Committed Access Rate |
| CBS | Committed Burst Size |
| CBQ | Class Based Queuing |
| CBR | Constant Bit Rate |
| CBT | Core-Based Tree |
| CCITT | International Telephone and Telegraph Consultative Committee |
| CE | Customer Edge |
| CFD | Connectivity Fault Detection |
| CFM | Configuration File Management |
| CHAP | Challenge Handshake Authentication Protocol |
| CIDR | Classless Inter-Domain Routing |
| CIR | Committed Information Rate |
| CIST | Common and Internal Spanning Tree |
| CLNP | Connectionless Network Protocol |
| CPOS | Channelized POS |
| CPU | Central Processing Unit |
| CQ | Custom Queuing |
| CRC | Cyclic Redundancy Check |
| CR-LSP | Constraint-based Routing LSP |
| CR-LDP | Constraint-based Routing LDP |
| CSMA/CD | Carrier Sense Multiple Access/Collision Detect |
| CSNP | Complete SNP |
| CSPF | Constraint Shortest Path First |
| CST | Common Spanning Tree |
| CT | Call Transfer |

| Acronyms | Full spelling |
| --- | --- |
| CV | Connectivity Verification |
| **D** | Return |
| DAR | Deeper Application Recognition |
| DCE | Data Circuit-terminal Equipment |
| DD | Database Description |
| DDN | Digital Data Network |
| DHCP | Dynamic Host Configuration Protocol |
| DIS | Designated IS |
| DLCI | Data Link Connection Identifier |
| DLDP | Device Link Detection Protocol |
| DNS | Domain Name System |
| DoD | Downstream on Demand |
| DoS | Denial of Service |
| DR | Designated Router |
| DSCP | Differentiated Services Codepoint Priority |
| DSP | Digital Signal Processor |
| DTE | Data Terminal Equipment |
| DU | Downstream Unsolicited |
| D-V | Distance Vector Routing Algorithm |
| DVMRP | Distance Vector Multicast Routing Protocol |
| DWDM | Dense Wavelength Division Multiplexing |
| **E** | Return |
| EACL | Enhanced ACL |
| EAD | Endpoint Admission Defense |
| EAP | Extensible Authentication Protocol |
| EAPOL | Extensible Authentication Protocol over LAN |
| EBGP | External Border Gateway Protocol |
| EBS | Excess Burst Size |
| EGP | Exterior Gateway Protocol |
| ES | End System |
| ES-IS | End System-Intermediate System |
| **F** | Return |
| FCoE | Fabric Channel over Ethernet |
| FC | Forwarding Class |
| FCS | Frame Check Sequence |
| FDDI | Fiber Distributed Data Interface |

| Acronyms | Full spelling |
| --- | --- |
| FDI | Forward Defect Indication |
| FEC | Forwarding Equivalence Class |
| FFD | Fast Failure Detection |
| FG | Forwarding Group |
| FIB | Forwarding information base |
| FIFO | First In First Out |
| FQDN | Full Qualified Domain Name |
| FR | Frame Relay |
| FRR | Fast ReRoute |
| FRTT | Fairness Round Trip Time |
| FT | Functional Test |
| FTP | File Transfer Protocol |
| **G** | Return |
| GARP | Generic Attribute Registration Protocol |
| GE | Gigabit Ethernet |
| GR | Graceful Restart |
| GRE | Generic Routing Encapsulation |
| GTS | Generic Traffic Shaping |
| GVRP | GARP VLAN Registration Protocol |
| **H** | Return |
| HA | High Availability |
| HABP | HW Authentication Bypass Protocol |
| HDLC | High-level Data Link Control |
| HEC | Header Error Control |
| HoPE | Hiberarchy of PE |
| HoVPN | Hiberarchy of VPN |
| HQoS | Hierarchical Quality of Service |
| HSB | Hot Standby |
| HTTP | Hyper Text Transport Protocol |
| H-VPLS | Hiberarchy of VPLS |
| HVRP | Hierarchy VLAN Register Protocol |
| HWTACACS | HUAWEI Terminal Access Controller Access Control System |
| **I** | Return |
| IA | Incoming Access |
| IANA | Internet Assigned Number Authority |
| IBGP | Internal BGP |

| Acronyms | Full spelling |
|---|---|
| IBM | International Business Machines |
| ICMP | Internet Control Message Protocol |
| ICMPv6 | Internet Control Message Protocol for IPv6 |
| ID | IDentification/IDentity |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IGMP | Internet Group Management Protocol |
| IGMP-Snooping | Internet Group Management Protocol Snooping |
| IGP | Interior Gateway Protocol |
| ILM | Incoming Label Map |
| ILS | Internet Locator Service |
| IN | Intelligent Network |
| IP | Internet Protocol |
| IPng | IP Next Generation |
| IPSec | IP Security |
| IPTN | IP Phone Telephony Network |
| IPv6 | Internet protocol version 6 |
| IPX | Internet Packet Exchange |
| IS | Intermediate System |
| ISATAP | Intra-Site Automatic Tunnel Addressing Protocol |
| ISDN | Integrated Services Digital Network |
| IS-IS | Intermediate System-to-Intermediate System intra-domain routing information exchange protocol |
| ISO | International Organization for Standardization |
| ISP | Internet service provider |
| ISSU | In Service Software Upgrade |
| IST | Internal Spanning Tree |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector |
| **K** | Return |
| KB | Kilobyte |
| KEK | Key-encrypting key |
| **L** | Return |
| L2TP | Layer 2 Tunneling Protocol |
| L2VPN | Layer 2 VPN |
| L3VPN | Layer 3 VPN |
| LACP | Link Aggregation Control Protocol |

| Acronyms | Full spelling |
|---|---|
| LACPDU | Link Aggregation Control Protocol Data Unit |
| LAN | Local Area Network |
| LCP | Link Control Protocol |
| LDAP | Lightweight Directory Access Protocol |
| LDP | Label Distribution Protocol |
| LER | Label Edge Router |
| LFIB | Label Forwarding Information Base |
| LIB | Label Information Base |
| LLC | Link Layer Control |
| LLDP | Link Layer Discovery Protocol |
| LOC | Loss of continuity |
| LOG | Call Logging |
| LR | Line Rate |
| LRTT | Loop Round Trip Time |
| LSA | Link State Advertisement |
| LSAck | Link State Acknowledgment |
| LSDB | Link State Database |
| LSP | Label Switch Path |
| LSPAGENT | Label Switched Path AGENT |
| LSPDU | Link State Protocol Data Unit |
| LSPM | Label Switch Path Management |
| LSR | Link State Request |
| LSR | Label Switch Router |
| LSR-ID | Label Switch Router Identity |
| LSU | Link State Update |
| **M** | **Return** |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| MaxBC | Max Bandwidth Constraints |
| MBGP | Multiprotocol Border Gateway Protocol |
| MD | Multicast Domain |
| MDI | Medium Dependent Interface |
| MDT | Multicast Distribution Tree |
| MED | multi-exit discrimination (MED) |
| MIB | Management Information Base |
| MLD | Multicast Listener Discovery Protocol |

| Acronyms | Full spelling |
| --- | --- |
| MLD-Snooping | Multicast Listener Discovery Snooping |
| MMC | Meet-Me Conference |
| MODEM | MOdulator-DEModulator |
| MP | Multilink PPP |
| MP-BGP | Multiprotocol extensions for BGP-4 |
| MPE | Middle-level PE |
| MP-group | Multilink Point to Point Protocol group |
| MPLS | Multiprotocol Label Switching |
| MPLSFW | Multi-protocol Label Switch Forward |
| MPM | Multicast Port Management |
| MSC | Mobile Switching Center |
| MSDP | Multicast Source Discovery Protocol |
| MSOH | Multiplex Section Overhead |
| MSTI | Multi-Spanning Tree Instance |
| MSTP | Multiple Spanning Tree Protocol |
| MT | Multicast Tunnel |
| MTBF | Mean Time Between Failure |
| MTI | Multicast Tunnel Interface |
| MTU | Maximum Transmission Unit |
| MVRF | Multicast VPN Routing and Forwarding |
| **N** | Return |
| NAPT | Network Address Port Translation |
| NAS | Network Access Server |
| NAT | Net Address Translation |
| NBMA | Non Broadcast Multi-Access |
| NBT | NetBIOS over TCP/IP |
| NCP | Network Control Protocol |
| ND | Neighborhood discovery |
| NDA | NetStream Data Analyzer |
| NDC | Network Data Collector |
| NDP | Neighbor Discovery Protocol |
| NetBIOS | Network Basic Input/Output System |
| NHLFE | Next Hop Label Forwarding Entry |
| NLPID | Network Layer Protocol Identifier |
| NLRI | Network Layer Reachable Information |
| NMS | Network Management Station |

| Acronyms | Full spelling |
| --- | --- |
| NPDU | Network Protocol Data Unit |
| NPE | Network Provider Edge |
| NQA | Network Quality Analyzer |
| NSAP | Network Service Access Point |
| NSC | NetStream Collector |
| N-SEL | NSAP Selector |
| NSSA | Not-So-Stubby Area |
| NTDP | Neighbor Topology Discovery Protocol |
| NTP | Network Time Protocol |
| **O** | Return |
| OAM | Operation Administration and Maintenance |
| OAMPDU | OAM Protocol Data Units |
| OC-3 | OC-3 |
| OID | Object Identifier |
| OL | Optical Line |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| **P** | Return |
| P2MP | Point to MultiPoint |
| P2P | Point To Point |
| PAP | Password Authentication Protocol |
| PCB | Printed Circuit Board |
| PCM | Pulse Code Modulation |
| PD | Powered Device |
| PDU | Protocol Data Unit |
| PE | Provider Edge |
| PHP | Penultimate Hop Popping |
| PHY | Physical layer |
| PIM | Protocol Independent Multicast |
| PIM-DM | Protocol Independent Multicast-Dense Mode |
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| PIR | Peak Information Rate |
| PKCS | Public Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| PMTU | Path MTU |
| PoE | Power over Ethernet |

| Acronyms | Full spelling |
|---|---|
| POP | Point Of Presence |
| POS | Packet Over SDH |
| PPP | Point-to-Point Protocol |
| PPTP | Point to Point Tunneling Protocol |
| PPVPN | Provider-provisioned Virtual Private Network |
| PQ | Priority Queuing |
| PRC | Primary Reference Clock |
| PRI | Primary Rate Interface |
| PS | Protection Switching |
| PSE | Power Sourcing Equipment |
| PSNP | Partial SNP |
| PVC | Permanent Virtual Channel |
| PW | Pseudo wires |
| **Q** | Return |
| QACL | QoS/ACL |
| QinQ | 802.1Q in 802.1Q |
| QoS | Quality of Service |
| QQIC | Querier's Query Interval Code |
| QRV | Querier's Robustness Variable |
| **R** | Return |
| RA | Registration Authority |
| RADIUS | Remote Authentication Dial in User Service |
| RAM | random-access memory |
| RD | Routing Domain |
| RD | Router Distinguisher |
| RED | Random Early Detection |
| RFC | Request For comments |
| RIP | Routing Information Protocol |
| RIPng | RIP next generation |
| RM | Route management |
| RMON | Remote Monitoring |
| ROM | Read Only Memory |
| RP | Rendezvous Point |
| RPC | Remote Procedure Call |
| RPF | Reverse Path Forwarding |
| RPR | Resilient Packet Ring |

| Acronyms | Full spelling |
| --- | --- |
| RPT | Rendezvous Point Tree |
| RRPP | Rapid Ring Protection Protocol |
| RSB | Reservation State Block |
| RSOH | Regenerator Section Overhead |
| RSTP | Rapid Spanning Tree Protocol |
| RSVP | Resource ReserVation Protocol |
| RTCP | Real-time Transport Control Protocol |
| RTE | Route Table Entry |
| RTP | Real-time Transport Protocol |
| RTP | Real-time Transport Protocol |
| **S** | **Return** |
| SA | Source Active |
| SBM | Subnetwork Bandwidth Management |
| SCFF | Single Choke Fairness Frame |
| SD | Signal Degrade |
| SDH | Synchronous Digital Hierarchy |
| SETS | Synchronous Equipment Timing Source |
| SF | Sampling Frequency |
| SFM | Source-Filtered Multicast |
| SFTP | Secure FTP |
| Share-MDT | Share-Multicast Distribution Tree |
| SIP | Session Initiation Protocol |
| Site-of-Origin | Site-of-Origin |
| SLA | Service Level Agreement |
| SMB | Standby Main Board |
| SMTP | Simple Mail Transfer Protocol |
| SNAP | Sub Network Access Point |
| SNMP | Simple Network Management Protocol |
| SNP | Sequence Number Packet |
| SNPA | Subnetwork Points of Attachment |
| SOH | Section Overhead |
| SONET | Synchronous Optical NETwork |
| SOO | Site-of-Origin |
| SP | Strict Priority Queueing |
| SPE | Superstratum PE/Sevice Provider-end PE |
| SPF | Shortest Path First |

| Acronyms | Full spelling |
|---|---|
| SPT | Shortest Path Tree |
| SSH | Secure Shell |
| SSM | Synchronization Status Marker |
| SSM | Source-Specific Multicast |
| ST | Shared Tree |
| STM-1 | SDH Transport Module -1 |
| STM-16 | SDH Transport Module -16 |
| STM-16c | SDH Transport Module -16c |
| STM-4c | SDH Transport Module -4c |
| STP | Spanning Tree Protocol |
| SVC | Signalling Virtual Connection |
| Switch-MDT | Switch-Multicast Distribution Tree |
| **T** | Return |
| TA | Terminal Adapter |
| TACACS | Terminal Access Controller Access Control System |
| TDM | Time Division Multiplexing |
| TCP | Transmission Control Protocol |
| TE | Traffic Engineering |
| TEDB | TE DataBase |
| TFTP | Trivial File Transfer Protocol |
| TLS | Transparent LAN Service |
| TLV | Type-Length-Value |
| ToS | Type of Service |
| TPID | Tag Protocol Identifier |
| TRIP | Trigger RIP |
| TS | Traffic Shaping |
| TTL | Time to Live |
| TTY | True Type Terminal |
| **U** | Return |
| UDP | User Datagram Protocol |
| UPE | Underlayer PE or User-end PE |
| URL | Uniform Resource Locators |
| URPF | Unicast Reverse Path Forwarding |
| USM | User-Based Security Model |
| **V** | Return |
| VBR | Variable Bit Rate |

| Acronyms | Full spelling |
| --- | --- |
| VCI | Virtual Channel Identifier |
| VE | Virtual Ethernet |
| VFS | Virtual File System |
| VLAN | Virtual Local Area Network |
| VLL | Virtual Leased Lines |
| VOD | Video On Demand |
| VoIP | Voice over IP |
| VOS | Virtual Operate System |
| VPDN | Virtual Private Dial-up Network |
| VPDN | Virtual Private Data Network |
| VPI | Virtual Path Identifier |
| VPLS | Virtual Private Local Switch |
| VPN | Virtual Private Network |
| VRID | Virtual Router ID |
| VRRP | Virtual Router Redundancy Protocol |
| VSI | Virtual Switch Interface |
| VT | Virtual Tributary |
| VTY | Virtual Type Terminal |
| **W** | Return |
| WAN | Wide Area Network |
| WFQ | Weighted Fair Queuing |
| WINS | Windows Internet Naming Service |
| WLAN | wireless local area network |
| WRED | Weighted Random Early Detection |
| WRR | Weighted Round Robin |
| WTR | Wait-to-Restore |
| WWW | World Wide Web |
| **X** | Return |
| XGE | Ten-GigabitEthernet |
| **Z** | Return |
| ZBR | Zone Border Router |

# Access Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The Access Volume is organized as follows:

| Features | Description |
|---|---|
| Ethernet Interface | This document describes:<br>• Combo Port Configuration<br>• Basic Ethernet Interface Configuration<br>• Configuring Flow Control on an Ethernet Interface<br>• Configuring the Suppression Time of Physical-Link-State Change on an Ethernet Interface<br>• Configuring Loopback Testing on an Ethernet Interface<br>• Configuring a Port Group<br>• Configuring Storm Suppression<br>• Setting the Interval for Collecting Ethernet Interface Statistics<br>• Enabling Forwarding of Jumbo Frames<br>• Enabling Loopback Detection on an Ethernet Interface<br>• Configuring the MDI Mode for an Ethernet Interface<br>• Testing the Cable on an Ethernet Interface<br>• Configuring the Storm Constrain Function on an Ethernet Interface |
| Link aggregation | Link aggregation aggregates multiple physical Ethernet ports into one logical link. This document describes:<br>• Basic Concepts of Link Aggregation<br>• Configuring a Static Aggregation Group<br>• Configuring a Dynamic Aggregation Group<br>• Configuring an Aggregate Interface<br>• Configuring a Load Sharing Mode for Load-Sharing Link Aggregation Groups |
| Port Isolation | The port isolation feature allows you to isolate different ports within the same VLAN. This document describes:<br>• Introduction to Port Isolation<br>• Configuring the Isolation Group |

| Features | Description |
| --- | --- |
| DLDP | In the use of fibers, link errors, namely unidirectional links, are likely to occur. DLDP is designed to detect such errors. This document describes:<br>• DLDP Introduction<br>• Enabling DLDP<br>• Setting DLDP Mode<br>• Setting the Interval for Sending Advertisement Packets<br>• Setting the DelayDown Timer<br>• Setting the Port Shutdown Mode<br>• Configuring DLDP Authentication<br>• Resetting DLDP State |
| LLDP | LLDP enables a device to maintain and manage its own and its immediate neighbor's device information, based on which the network management system detects and determines the conditions of the communications links. This document describes:<br>• Introduction to LLDP<br>• Performing Basic LLDP Configuration<br>• Configuring the Encapsulation Format for LLDPDUs<br>• Configuring the Encapsulation Format of the Management Address<br>• Configuring CDP Compatibility<br>• Configuring LLDP Trapping |
| MSTP | MSTP is used to eliminate loops in a LAN. It is compatible with STP and RSTP. This document describes:<br>• Introduction to MSTP<br>• Configuring the Root Bridge<br>• Configuring Leaf Nodes<br>• Performing mCheck<br>• Configuring Digest Snooping<br>• Configuring No Agreement Check<br>• Configuring Protection Functions |
| Smart Link | Smart Link is a solution for active-standby link redundancy backup and rapid transition in dual-uplink networking. This document describes:<br>• Smart Link Overview<br>• Configuring a Smart Link Device<br>• Configuring an Associated Device |
| Monitor Link | Monitor link is a port collaboration function used to enable a device to be aware of the up/down state change of the ports on an indirectly connected link. This document describes:<br>• Monitor Link Overview<br>• Configuring Monitor Link |
| VLAN | Using the VLAN technology, you can partition a LAN into multiple logical LANs. This document describes:<br>• Introduction to VLAN<br>• Types of VLAN<br>• Isolate-user-vlan configuration<br>• Introduction and Configuration of Voice VLAN |

| Features | Description |
| --- | --- |
| GVRP | GVRP is a GARP application. This document describes:<br>• GARP overview<br>• GVRP configuration<br>• GARP Timers configuration |
| QinQ | As defined in IEEE802.1Q, 12 bits are used to identify a VLAN ID, so a device can support a maximum of 4094 VLANs. The QinQ feature extends the VLAN space by allowing Ethernet frames to travel across the service provider network with double VLAN tags. This document describes:<br>• Introduction to QinQ<br>• Configuring basic QinQ<br>• Configuring Selective QinQ<br>• Configuring the TPID Value in VLAN Tags |
| BPDU Tunnel | BPDU tunneling enables transparently transmission of customer network BPDU frames over the service provider network. This document describes:<br>• Introduction to BPDU Tunneling<br>• Configuring BPDU Transparent Transmission<br>• Configuring Destination Multicast MAC Address for BPDU Tunnel Frames |
| Ethernet OAM | Ethernet OAM is a tool monitoring Layer-2 link status. It helps network administrators manage their networks effectively. This document describes:<br>• Ethernet OAM overview<br>• Configuring Basic Ethernet OAM Functions<br>• Configuring Link Monitoring<br>• Enabling OAM Loopback Testing |
| Connectivity Fault Detection | Connectivity fault detection is an end-to-end, per-VLAN link-layer OAM mechanism for link connectivity detection, fault verification, and fault location. This document describes:<br>• Connectivity Fault Detection Overview<br>• Basic Configuration Tasks<br>• Configuring CC on MEPs<br>• Configuring LB on MEPs<br>• Configuring LT on MEPs |
| RRPP | RRPP is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes after a link is disconnected on the ring. This document describes:<br>• RRPP overview<br>• Configuring Master Node<br>• Configuring Transit Node<br>• Configuring Edge Node<br>• Configuring Assistant Edge Node<br>• Configuring Ring Group |

| Features | Description |
| --- | --- |
| Port Mirroring | Port mirroring copies packets passing through a port to another port connected with a monitoring device for packet analysis to help implement network monitoring and troubleshooting. This document describes:<br>• Port Mirroring overview<br>• Local port mirroring configuration<br>• Remote port mirroring configuration |

# Table of Contents

# 1 Ethernet Interface Configuration

## General Ethernet Interface Configuration

### Combo Port Configuration

#### Introduction to Combo port

A Combo port can operate as either an optical port or an electrical port. Inside the device there is only one forwarding interface. For a Combo port, the electrical port and the corresponding optical port are TX-SFP multiplexed. You can specify a Combo port to operate as an electrical port or an optical port. That is, a Combo port cannot operate as both an electrical port and an optical port simultaneously. When one is enabled, the other is automatically disabled.

#### Configuring Combo port state

Follow these steps to configure the state of a Combo port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Enable a specified Combo port | **undo shutdown** | Optional<br>By default, of the two ports in a Combo port, the one with a smaller port ID is enabled. |

**Note**

In case of a Combo port, only one interface (either the optical port or the electrical port) is active at a time. That is, once the optical port is active, the electrical port will be inactive automatically, and vice versa.

### Basic Ethernet Interface Configuration

#### Configuring an Ethernet interface

Three types of duplex modes are available to Ethernet interfaces:

- Full-duplex mode (full). Interfaces operating in this mode can send and receive packets simultaneously.
- Half-duplex mode (half). Interfaces operating in this mode can either send or receive packets at a given time.

- Auto-negotiation mode (auto). Interfaces operating in this mode determine their duplex mode through auto-negotiation.

Similarly, if you configure the transmission rate for an Ethernet interface by using the **speed** command with the **auto** keyword specified, the transmission rate is determined through auto-negotiation too. For a Gigabit Ethernet interface, you can specify the transmission rate by its auto-negotiation capacity.

Follow these steps to configure an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Set the description string | **description** *text* | Optional<br>By default, the description of an interface is the interface name followed by the "interface" string, **GigabitEthernet1/0/1 Interface** for example. |
| Set the duplex mode | **duplex** { **auto** \| **full** \| **half** } | Optional<br>**auto** by default.<br>The optical interface of a Combo port does not support the **half** keyword. |
| Set the transmission rate | **speed** { **10** \| **100** \| **1000** \| **auto** } | Optional<br>The optical interface of a Combo port does not support the **10** or **100** keyword.<br>By default, the port speed is in the auto-negotiation mode. |
| Shut down the Ethernet interface | **shutdown** | Optional<br>By default, an Ethernet interface is in up state.<br>To bring up an Ethernet interface, use the **undo shutdown** command. |

**Note**

10-Gigabit Ethernet ports do not support the **duplex** command or the **speed** command.

## Configuring Flow Control on an Ethernet Interface

When flow control is enabled on both sides, if traffic congestion occurs at the ingress interface, it will send a Pause frame notifying the egress interface to temporarily suspend the sending of packets. The egress interface is expected to stop sending any new packet when it receives the Pause frame. In this way, flow control helps to avoid dropping of packets. Note that this will be possible only after flow control is enabled on both the ingress and egress interfaces.

Follow these steps to enable flow control on an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Enable flow control | **flow-control** | Required<br>Disabled by default |

## Configuring the Suppression Time of Physical-Link-State Change on an Ethernet Interface

An Ethernet interface operates in one of the two physical link states: up or down. During the suppression time, physical-link-state changes will not be propagated to the system. Only after the suppression time has elapsed will the system be notified of the physical-link-state changes by the physical layer. This functionality reduces the extra overhead occurred due to frequent physical-link-state changes within a short period of time.

Follow these steps to configure the suppression time of physical-link-state changes on an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Configure the up/down suppression time of physical-link-state changes | **link-delay** *delay-time* | Required<br>By default, the physical-link-state change suppression time is not configured. |

## Configuring Loopback Testing on an Ethernet Interface

You can enable loopback testing to check whether the Ethernet interface functions properly. Note that no data packets can be forwarded during the testing. Loopback testing falls into the following two categories:

- Internal loopback testing, which is performed within switching chips to test the functions related to the Ethernet interfaces.
- External loopback testing, which is used to test the hardware functions of an Ethernet interface. To perform external loopback testing on an Ethernet interface, you need to install a loopback plug on the Ethernet interface. In this case, packets sent from the interface are received by the same interface.

Follow these steps to enable Ethernet interface loopback testing:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable loopback testing | **loopback** { **external** \| **internal** } | Optional<br>Disabled by default. |

**Note**

- As for the internal loopback test and external loopback test, if an interface is down, only the former is available on it; if the interface is shut down, both are unavailable.
- The **speed**, **duplex**, **mdi**, and **shutdown** commands are not applicable during loopback testing.
- With the loopback testing enabled, the Ethernet interface operates in full duplex mode. With the loopback testing disabled, the original configurations will be restored.

## Configuring a Port Group

The devices allow you to configure some functions on multiple interfaces at a time by assigning the interfaces to a port group in addition to configuring them on a per-interface basis. This is helpful when you have to configure a feature in the same way on multiple interfaces.

A port group is created manually and the settings you made on it apply to all group member interfaces. Note that even though the settings are made on the port group, they are saved on an interface basis rather than on a port group basis. Thus, you can only view the settings in the view of each interface with the **display current-configuration** command or the **display this** command.

Follow these steps to configure a manual port group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a manual port group and enter manual port group view | **port-group manual** *port-group-name* | Required |
| Add Ethernet interfaces to the manual port group | **group-member** *interface-list* | Required |

## Configuring Storm Suppression

You can use the following commands to suppress the broadcast, multicast, and unknown unicast traffic. In interface configuration mode, the suppression ratio indicates the maximum broadcast, multicast or unknown unicast traffic that is allowed to pass through an interface. When the broadcast, multicast, or unknown unicast traffic over the interface exceeds the threshold, the system will discard the extra packets so that the broadcast, multicast or unknown unicast traffic ratio can drop below the limit to ensure that the network functions properly.

**Note**

The storm suppression ratio settings configured for an Ethernet interface may get invalid if you enable the storm constrain for the interface. For information about the storm constrain function, see Configuring the Storm Constrain Function on an Ethernet Interface.

Follow these steps to set storm suppression ratios for one or multiple Ethernet interfaces:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Use either command.<br>If configured in Ethernet interface view, this feature takes effect on the current port only; if configured in port group view, this feature takes effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Set the broadcast storm suppression ratio | | **broadcast-suppression** { *ratio* \| **pps** *max-pps* } | Optional<br>By default, all broadcast traffic is allowed to pass through an interface, that is, broadcast traffic is not suppressed. |
| Set the multicast storm suppression ratio | | **multicast-suppression** { *ratio* \| **pps** *max-pps* } | Optional<br>By default, all multicast traffic is allowed to pass through an interface, that is, multicast traffic is not suppressed. |
| Set the unknown unicast storm suppression ratio | | **unicast-suppression** { *ratio* \| **pps** *max-pps* } | Optional<br>By default, all unknown unicast traffic is allowed to pass through an interface, that is, unknown unicast traffic is not suppressed. |

**Note**

If you set storm suppression ratios in Ethernet interface view or port group view repeatedly for an Ethernet interface that belongs to a port group, only the latest settings take effect.

## Setting the Interval for Collecting Ethernet Interface Statistics

Follow these steps to configure the interval for collecting interface statistics:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the interval for collecting interface statistics | **interface** *interface-type interface-number* | Optional<br>The default interval for collecting interface statistics is 300 seconds. |
| | **flow-interval** *interval* | |

## Enabling Forwarding of Jumbo Frames

Due to tremendous amount of traffic occurring on an Ethernet interface, it is likely that some frames greater than the standard Ethernet frame size are received. Such frames (called jumbo frames) will be dropped. With forwarding of jumbo frames enabled, the system does not drop all the jumbo frames. Instead, it continues to process jumbo frames with a size greater than the standard Ethernet frame size and yet within the specified parameter range.

In interface configuration mode (Ethernet interface view/port-group view), you can set the length of jumbo frames that can pass through the Ethernet interface.

- If you execute the command in Ethernet interface view, the configurations take effect only on the current interface.
- If you execute the command in port-group view, the configurations take effect on all ports in the port group.

Follow these steps to enable the forwarding of jumbo frames:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable the forwarding of jumbo frames | In port-group view | **port-group manual** *port-group-name* | Use any command.<br>By default, the device allows jumbo frames with the length of 9.216 bytes to pass through all Layer 2 Ethernet interfaces. |
| | | **jumboframe enable** | |
| | In Ethernet interface view | **interface** *interface-type interface-number* | |
| | | **jumboframe enable** | |

## Enabling Loopback Detection on an Ethernet Interface

If a port receives a packet that it sent out, a loop occurs. Loops may cause broadcast storms. The purpose of loopback detection is to detect loops on an interface.

When loopback detection is enabled on an Ethernet interface, the device periodically checks whether the ports have any external loopback. If it detects a loopback on a port, the device will set that port to be under loopback detection mode.

- If loops are detected on an access port, the port will be blocked. Meanwhile, trap messages will be sent to the terminal, and the corresponding MAC address forwarding entries will be removed.
- If loops are detected on a trunk port or a hybrid port, trap messages are sent to the terminal. If the loopback detection control function is also enabled on the port, the port will be blocked, trap

messages will be sent to the terminal, and the corresponding MAC address forwarding entries will be removed.

Follow these steps to configure loopback detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable global loopback detection | **loopback-detection enable** | Required<br>Disabled by default |
| Configure the interval for port loopback detection | **loopback-detection interval-time** *time* | Optional<br>30 seconds by default |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Enable loopback detection on a port | **loopback-detection enable** | Required<br>Disabled by default |
| Enable loopback detection control on a trunk port or a hybrid port | **loopback-detection control enable** | Optional<br>Disabled by default |
| Enable loopback detection in all the VLANs to which trunk or hybrid ports belong | **loopback-detection per-vlan enable** | Optional<br>Enabled only in the default VLAN(s) with trunk port or hybrid ports |

**Caution**

- Loopback detection on a given port is enabled only after the **loopback-detection enable** command has been configured in both system view and the interface view of the port.
- Loopback detection on all ports will be disabled after the configuration of the **undo loopback-detection enable** command under system view.

## Configuring the MDI Mode for an Ethernet Interface

**Note**

10-Gigabit Ethernet ports and combo ports operating as optical interfaces do not support this function.

Two types of Ethernet cables can be used to connect Ethernet devices: crossover cable and straight-through cable. To accommodate these two types of cables, an Ethernet interface on a device can operate in one of the following three Medium Dependent Interface (MDI) modes:

- Across mode
- Normal mode
- Auto mode

An Ethernet interface is composed of eight pins. By default, each pin has its particular role. For example, pin 1 and pin 2 are used for transmitting signals; pin 3 and pin 6 are used for receiving signals. You can change the pin roles through setting the MDI mode. For an Ethernet interface in normal mode, the pin roles are not changed. For an Ethernet interface in across mode, pin 1 and pin 2 are used for receiving signals; pin 3 and pin 6 are used for transmitting signals. To enable normal communication, you should connect the local transmit pins to the remote receive pins. Therefore, you should configure the MDI mode depending on the cable types.

- Normally, the auto mode is recommended. The other two modes are useful only when the device cannot determine the cable type.
- When straight-through cables are used, the local MDI mode must be different from the remote MDI mode.
- When crossover cables are used, the local MDI mode must be the same as the remote MDI mode, or the MDI mode of at least one end must be set to **auto**.

Follow these steps to configure the MDI mode for an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Configure the MDI mode for the Ethernet interface | **mdi** { **across** \| **auto** \| **normal** } | Optional<br>Defaults to **auto**. That is, the Ethernet interface determines the physical pin roles (transmit or receive) through negotiation. |

## Testing the Cable on an Ethernet Interface

**Note**

- 10-Gigabit Ethernet ports and Combo ports operating as optical interfaces do not support this feature.
- A link in the up state goes down and then up automatically if you perform the operation described in this section on one of the Ethernet interfaces forming the link.

Follow these steps to test the current operating state of the cable connected to an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Test the cable connected to the Ethernet interface once | **virtual-cable-test** | Required |

## Configuring the Storm Constrain Function on an Ethernet Interface

The storm constrain function suppresses packet storms in an Ethernet. With this function enabled on an interface, the system detects the multicast traffic, or broadcast traffic passing through the interface periodically and takes corresponding actions (that is, blocking or shutting down the interface and sending trap messages and logs) when the traffic detected exceeds the threshold.

---

**Caution**

Alternatively, you can configure the storm suppression function to control a specific type of traffic. As the function and the storm constrain function are mutually exclusive, do not enable them at the same time on an Ethernet interface. For example, with broadcast storm suppression ratio set on an Ethernet interface, do not enable the storm constrain function for broadcast traffic on the interface. Refer to Configuring Storm Suppression for information about the storm suppression function.

---

With the storm constrain function enabled on an Ethernet interface, you can specify the system to act as follows when the traffic detected exceeds the threshold.

- Blocking the interface. In this case, the interface is blocked and thus stops forwarding the traffic of this type till the traffic detected is lower than the threshold. Note that an interface blocked by the storm constrain function can still forward other types of traffic and monitor the blocked traffic.
- Shutting down the interface. In this case, the interface is shut down and stops forwarding all types of traffic. Interfaces shut down by the storm constrain function can only be brought up by using the **undo shutdown** command or disabling the storm constrain function.

Follow these steps to configure the storm constrain function on an Ethernet interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the interval for generating traffic statistics | **storm-constrain interval** *seconds* | Optional<br>10 seconds by default |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Enable the storm constrain function and set the lower threshold and the upper threshold | **storm-constrain** { **broadcast** \| **multicast** } { **pps** \| **kbps** \| **ratio** } *max-pps-values min-pps-values* | Required<br>Disabled by default |
| Set the action to be taken when the traffic exceeds the upper threshold | **storm-constrain control** { **block** \| **shutdown** } | Optional<br>Disabled by default |
| Specify to send trap messages when the traffic detected exceeds the upper threshold or drops down below the lower threshold from a point higher than the upper threshold | **storm-constrain enable trap** | Optional<br>By default, the system sends trap messages when the traffic detected exceeds the upper threshold or drops down below the lower threshold from a point higher than the upper threshold. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify to send log when the traffic detected exceeds the upper threshold or drops down below the lower threshold from a point higher than the upper threshold | **storm-constrain enable log** | Optional<br>By default, the system sends log when the traffic detected exceeds the upper threshold or drops down below the lower threshold from a point higher than the upper threshold. |

**Note**

- For network stability sake, configure the interval for generating traffic statistics to a value that is not shorter than the default.
- The storm constrain function, after being enabled, requires a complete statistical period (specified by the storm-constrain interval command) to collect traffic data, and analyzes the data in the next period. Thus, it is normal that a period longer than one statistic period is waited for a control action to happen if you enable the function while the packet storm is present. However, the action will be taken within two periods.
- The storm constrain function is applicable to multicast packets, and broadcast packets; and you can specify the upper and lower threshold for any of the three types of packets.

## Displaying and Maintaining an Ethernet Interface

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current state of an interface/subinterface and the related information | **display interface** [ *interface-type* [ *interface-number* ] ] | Available in any view |
| Display the summary of an interface/subinterface | **display brief interface** [ *interface-type* [ *interface-number* ] ] [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | Available in any view |
| Display information about discarded packets on an interface | **display packet-drop interface** [ *interface-type* [ *interface-number* ] ] | Available in any view |
| Display summary information about discarded packets on all interfaces | **display packet-drop summary** | Available in any view |
| Clear the statistics of an interface/subinterface | **reset counters interface** [ *interface-type* [ *interface-number* ] ] | Available in user view |
| Clear the statistics of discarded packets on an interface | **reset packet-drop interface** [ *interface-type* [ *interface-number* ] ] | Available in user view |
| Display the Combo ports and the corresponding optical/electrical ports | **display port combo** | Available in any view |

| To do… | Use the command… | Remarks |
| --- | --- | --- |
| Display the information about a manual port group or all the port groups | **display port-group manual** [ **all** \| **name** *port-group-name* ] | Available in any view |
| Display the information about the loopback function | **display loopback-detection** | Available in any view |
| Display the information about storm constrain | **display storm-constrain** [ **broadcast** \| **multicast** ] [ **interface** *interface-type interface-number* ] | Available in any view |

# Table of Contents

# 1 Link Aggregation Configuration

When configuring link aggregation, go to these sections for information you are interested in:



## Overview

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group.

It allows you to increase bandwidth by distributing traffic across the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

### Basic Concepts of Link Aggregation

#### Aggregate interface

An aggregate interface is a logical Layer 2 or Layer-3 aggregate interface.

#### Aggregation group

An aggregation group is a collection of Ethernet interfaces. When you create an aggregate interface, an aggregation group numbered the same is created automatically depending on the type of the aggregate interface:

- If the aggregate interface is a Layer 2 interface, a Layer 2 aggregation group is created. You can assign only Layer 2 Ethernet interfaces to the group.
- If the aggregate interface is a Layer-3 interface, a Layer-3 aggregation group is created. You can assign only Layer-3 Ethernet interfaces to the group.

---

**Note**

The current device only supports Layer 2 aggregation groups.

---

#### States of the member ports in an aggregation group

A member port in an aggregation group can be in one of the following two states:

- Selected: a selected port can forward user traffic.
- Unselected: an unselected port cannot forward user traffic.

The rate of an aggregate interface is the sum of the selected member ports' rates. The duplex mode of an aggregate interface is consistent with that of the selected member ports. Note that all selected member ports use the same duplex mode.

For how the state of a member port is determined, refer to Static aggregation mode and Dynamic aggregation mode.

### LACP protocol

The Link Aggregation Control Protocol (LACP) is defined in IEEE 802.3ad. It uses link aggregation control protocol data units (LACPDUs) for information exchange between LACP-enabled devices.

LACP is automatically enabled on interfaces in a dynamic aggregation group. For information about dynamic aggregation groups, refer to Dynamic aggregation mode. An LACP-enabled interface sends LACPDUs to notify the remote system (the partner) of its system LACP priority, system MAC address, LACP port priority, port number, and operational key. Upon receiving an LACPDU, the partner compares the received information with the information received on other interfaces to determine the interfaces that can operate as selected interfaces. This allows the two systems to reach an agreement on which link aggregation member ports should be placed in selected state.

### Operational key

When aggregating ports, link aggregation control automatically assigns each port an operational key based on the port attributes, including the configurations of the port rate, duplex mode and link state.

In a link aggregation group, all member ports in the selected state have the same operation key.

### Class-two configurations

Class-two configurations are listed in Table 1-1. In an aggregation group, if the configurations of a member port are different from the class-two configurations, that member port cannot be a selected port.

**Table 1-1** Class-two configurations

| Type | Considerations |
|---|---|
| Port isolation | Whether a port has joined an isolation group, and the isolation group that the port belongs to |
| QinQ | QinQ enable state (enable/disable), outer VLAN tags to be added, inner-to-outer VLAN priority mappings, inner-to-outer VLAN tag mappings, inner VLAN ID substitution mappings |
| VLAN | Permitted VLAN IDs, default VLAN, link type (trunk, hybrid, or access), IP subnet-based VLAN configuration, protocol-based VLAN configuration, tag mode |
| MAC address learning | MAC address learning capability, MAC address learning limit, forwarding of frames with unknown destination MAC addresses after the upper limit of the MAC address table is reached |

**Note**

- Some configurations are called class-one configurations. Such configurations, for example, GVRP and MSTP, can be configured on aggregate interfaces and member ports but are not considered during operational key calculation.
- The change of a class-two configuration setting may affect the select state of link aggregation member ports and thus the ongoing service. To prevent unconsidered change, a message warning of the hazard will be displayed when you attempt to change a class-two setting, upon which you can decide whether to continue your change operation.

## Link Aggregation Modes

Depending on the link aggregation procedure, link aggregation operates in one of the following two modes:

- Static aggregation mode
- Dynamic aggregation mode

### Static aggregation mode

LACP is disabled on the member ports in a static aggregation group. In a static aggregation group, the system sets a port to selected or unselected state by the following rules:

- Select a port as the reference port from the ports that are in up state and with the same class-two configurations as the corresponding aggregate interface. These ports are selected in the order of full duplex/high speed, full duplex/low speed, half duplex/high speed, and half duplex/low speed, with full duplex/high speed being the most preferred. If two ports with the same duplex mode/speed pair are present, the one with the lower port number wins out.
- Consider the ports in up state with the same port attributes and class-two configurations as the reference port as candidate selected ports, and set all others in the unselected state.
- Static aggregation limits the number of selected ports in an aggregation group. When the number of the candidate selected ports is under the limit, all the candidate selected ports become selected ports. When the limit is exceeded, set the candidate selected ports with smaller port numbers in the selected state and those with greater port numbers in the unselected state.
- If all the member ports are down, set their states to unselected.
- Set the ports that cannot aggregate with the reference port to the unselected state.

**Caution**

A port that joins the aggregation group after the limit on the number of selected ports has been reached will not be placed in the selected state even if it should be in normal cases. This can prevent the ongoing traffic on the current selected ports from being interrupted. You should avoid the situation however, as this may cause the selected/unselected state of a port to change after a reboot.

### Dynamic aggregation mode

LACP is enabled on member ports in a dynamic aggregation group.

In a dynamic aggregation group,

- A selected port can receive and transmit LACPDUs.
- An unselected port can receive and send LACPDUs only if it is up and with the same configurations as those on the aggregate interface.

In a dynamic aggregation group, the system sets the ports to selected or unselected state in the following steps:

1) The local system (the actor) negotiates with the remote system (the partner) to determine port state based on the port IDs on the end with the preferred system ID. The following is the detailed negotiation procedure:

- Compare the system ID (comprising the system LACP priority and the system MAC address) of the actor with that of the partner. The system with the lower LACP priority wins out. If they are the same, compare the system MAC addresses. The system with the smaller MAC address wins out.
- Compare the port IDs of the ports on the system with the smaller system ID. A port ID comprises a port LACP priority and a port number. First compare the port LACP priorities. The port with the lower LACP priority wins out. If two ports are with the same LACP priority, compare their port numbers. The port with the smaller port ID, that is, the port with smaller port number, is selected as the reference port.
- If a port (in up state) is with the same port attributes and class-two configuration as the reference port, and the peer port of the port is with the same port attributes and class-two configurations as the peer port of the reference port, consider the port as a candidate selected port; otherwise set the port to the unselected state.
- The number of selected ports that an aggregation group can contain is limited. When the number of candidate selected ports is under the limit, all the candidate selected ports are set to selected state. When the limit is exceeded, the system selects the candidate selected ports with smaller port IDs as the selected ports, and set other candidate selected ports to unselected state. At the same time, the peer device, being aware of the changes, changes the state of its ports accordingly.

2) Set the ports that cannot aggregate with the reference port to the unselected state.

---

**Note**

For static and dynamic aggregation modes:

- In an aggregation group, the port to be a selected port must be the same as the reference port in port attributes, and class-two configurations. To keep these configurations consistent, you should configure the port manually.
- Because changing a port attribute or class-two configuration setting of a port may cause the select state of the port and other member ports to change and thus affects services, you are recommended to do that with caution.

---

## Load Sharing Mode of an Aggregation Group

A link aggregation groups operates in load sharing aggregation mode or non-load sharing mode.

The system sets the load sharing mode of an aggregation group as follows:

- When hardware resources are available, a link aggregation group with at least two selected ports operates in load sharing mode. The load sharing mode of a link aggregation group with only one selected port is non-load sharing mode.
- After hardware resources become depleted (a number of 128 link aggregation groups have been created in the system), all the link aggregation groups operate in non-load sharing mode.

---

 **Note**

- After you remove all ports but one selected port from a load-sharing aggregation group, the aggregation group remains to be a load sharing group.
- A load-sharing aggregation group contains at least one selected port while a non-load-sharing aggregation group can only have one selected port at most.
- After hardware resources become depleted, all new link aggregation groups operate in non-load sharing mode. They will not perform load sharing even after resources become available again for example after some aggregation groups are removed. To have them perform load sharing, you can re-enable their corresponding aggregation interfaces by shutting down and then bringing up the interfaces.

---

## Link Aggregation Configuration Task List

Complete the following tasks to configure link aggregation:

| Task | | Remarks |
|---|---|---|
| Configuring an Aggregation Group | Configuring a Static Aggregation Group | Required<br>Perform either of the tasks |
| | Configuring a Dynamic Aggregation Group | |
| Configuring an Aggregate Interface | Configuring the Description of an Aggregate Interface | Optional |
| | Enabling LinkUp/LinkDown Trap Generation for an Aggregate Interface | Optional |
| | Shutting Down an Aggregate Interface | Optional |
| Configuring a Load Sharing Mode for Load-Sharing Link Aggregation Groups | | Optional |

# Configuring an Aggregation Group

**Note**

- The following ports cannot be assigned to an aggregation group: Stack ports, RRPP-enabled ports, MAC address authentication-enabled ports, port security-enabled ports, IP source guard-enabled ports, and 802.1x-enabled ports.
- You are recommended not to assign reflector ports of port mirroring to an aggregation group. For details about reflector ports, refer to *Port Mirroring Configuration* in the *Access Volume*.

## Configuring a Static Aggregation Group

Follow these steps to configure a Layer 2 static aggregation group:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a Layer 2 aggregate interface and enter the Layer 2 aggregate interface view | **interface bridge-aggregation** *interface-number* | Required<br>When you create a Layer 2 aggregate interface, a Layer 2 static aggregation group numbered the same is created automatically. |
| Exit to system view | **quit** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Repeat the two steps to assign multiple Ethernet interfaces to the aggregation group. |
| Assign the Ethernet interface to the aggregation group | **port link-aggregation group** *number* | |

**Caution**

- Removing a Layer 2 aggregate interface also removes the corresponding aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.
- To guarantee a successful static aggregation, ensure that the ports at the two ends of each link to be aggregated are consistent in the selected/unselected state.

## Configuring a Dynamic Aggregation Group

Follow these steps to configure a Layer 2 dynamic aggregation group:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the system LACP priority | **lacp system-priority** *system-priority* | Optional<br>By default, the system LACP priority is 32768.<br>Changing the system LACP priority may affect the selected/unselected state of the ports in the dynamic aggregation group. |
| Create a Layer 2 aggregate interface and enter the Layer 2 aggregate interface view | **interface bridge-aggregation** *interface-number* | Required<br>When you create a Layer 2 aggregate interface, a Layer 2 static aggregation group numbered the same is created automatically. |
| Configure the aggregation group to work in dynamic aggregation mode | **link-aggregation mode dynamic** | Required<br>By default, an aggregation group works in static aggregation mode. |
| Exit to system view | **quit** | — |
| Enter Layer 2 Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Repeat the two steps to assign multiple Ethernet interfaces to the aggregation group. |
| Assign the Ethernet interface to the aggregation group | **port link-aggregation group** *number* | |
| Assign the port a LACP priority | **lacp port-priority** *port-priority* | Optional<br>By default, the LACP priority of a port is 32768.<br>Changing the LACP priority of a port may affect the selected/unselected state of the ports in the dynamic aggregation group. |

**Caution**

- Removing a dynamic aggregate interface also removes the corresponding aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.
- To guarantee a successful dynamic aggregation, ensure that the peer ports of the ports aggregated at one end are also aggregated. The two ends can automatically negotiate the selected state of the ports.
- When a load-sharing aggregation group becomes a non-load-sharing aggregation group because of insufficient load sharing resources, one of the following problems may occur: the number of selected ports of the actor is inconsistent with that of the partner, which may result in incorrect traffic forwarding; the peer port of a selected port is an unselected one, which may result in upper-layer protocol and traffic forwarding anomalies. You should fully consider the situation when making configuration.

# Configuring an Aggregate Interface

You can perform the following configurations for an aggregate interface:

- Configuring the Description of an Aggregate Interface
- Enabling LinkUp/LinkDown Trap Generation for an Aggregate Interface
- Shutting Down an Aggregate Interface

## Configuring the Description of an Aggregate Interface

Follow these steps to configure the description of an aggregate interface:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Layer 2 aggregate interface view | **interface bridge-aggregation** *interface-number* | — |
| Configure the description of the aggregate interface | **description** *text* | Optional<br>By default, the description of an interface is *interface-name* **Interface**, such as **Bridge-Aggregation1 Interface**. |

## Enabling LinkUp/LinkDown Trap Generation for an Aggregate Interface

To enable an aggregate interface to generate linkUp/linkDown trap messages when the state of the interface changes, you should enable linkUp/linkDown trap generation on the aggregate interface.

Follow these steps to enable linkUp/linkDown trap generation for an aggregate interface:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the trap function globally | **snmp-agent trap enable** [ **standard** [ **linkdown** \| **linkup** ] * ] | Optional<br>By default, linkUp/linkDown trap generation is enabled globally and on all interfaces. |
| Enter aggregate interface view | **interface bridge-aggregation** *interface-number* | — |
| Enable linkUp/linkDown trap generation for the aggregate interface | **enable snmp trap updown** | Optional<br>Enabled by default |

### Shutting Down an Aggregate Interface

Shutting down or bringing up an aggregate interface affects the selected state of the ports in the corresponding aggregation group. When an aggregate interface is shut down, all selected ports in its aggregation group become unselected; when the aggregate interface is brought up, the selected state of the ports in the corresponding aggregation group is re-calculated.

Follow these steps to shut down an aggregate interface:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Layer 2 aggregate interface view | **interface bridge-aggregation** *interface-number* | — |
| Shut down the aggregate interface | **shutdown** | Required<br>By default, aggregate interfaces are up. |

**Caution**

After shutting down an aggregate interface, you are recommended not to use the **shutdown** command and then the **undo shutdown** command on the member interfaces of the corresponding link aggregation group. Otherwise, the member interfaces may be brought up.

## Configuring a Load Sharing Mode for Load-Sharing Link Aggregation Groups

The hash algorithm is adopted to calculate load sharing for load-sharing link aggregation groups. Hash keys used for calculation could be service port numbers, IP addresses, MAC addresses, incoming ports, or any combinations of them. One hash key or a combination of multiple hash keys represents a load sharing mode. You can change the load sharing mode of a link aggregation group for different types of

traffic as needed. For example, for Layer 3 traffic, you can use IP addresses as hash keys for load sharing calculation.

Follow these steps to configure load sharing mode for link aggregation groups:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the link aggregation load sharing mode | **link-aggregation load-sharing mode** { **destination-ip** \| **destination-mac** \| **destination-port** \| **ingress-port** \| **source-ip** \| **source-mac** \| **source-port** } * | Optional<br>By default, the hash keys for Layer 2 packets are source/destination MAC addresses, and those for Layer-3 packets are source/destination IP addresses.<br>The setting you made applies to all load-sharing link aggregation groups. |

**Note**

Currently, the hash keys for a switch are source IP addresses, destination IP addresses, source MAC addresses, destination MAC addresses, source ports, destination ports, or the combination of these fields carried in packets (excluding the combination of MAC addresses with IP addresses, source ports, or destination ports). The **ingress-port** parameter can only be used as a hash key when combined with a MAC address, not when combined with an IP address, source port, or destination port. The parameter alone cannot be used as a hash key either.

## Displaying and Maintaining Link Aggregation

| To do... | Use the command... | Remarks |
|---|---|---|
| Display the local system ID | **display lacp system-id** | Available in any view |
| Display the aggregation group-specific load sharing mode | **display link-aggregation load-sharing mode** | Available in any view |
| Display link aggregation details of ports | **display link-aggregation member-port** [ *interface-type interface-number* [ **to** *interface-type interface-number* ] ] | Available in any view |
| Display the summary information of all aggregation groups | **display link-aggregation summary** | Available in any view |
| Display detailed information of aggregation groups | **display link-aggregation verbose** [ **bridge-aggregation** [ *interface-number* ] ] | Available in any view |
| Clear the LACP statistics of ports | **reset lacp statistics** [ **interface** *interface-type interface-number* [ **to** *interface-type interface-number* ] ] | Available in user view |

# Link Aggregation Configuration Examples

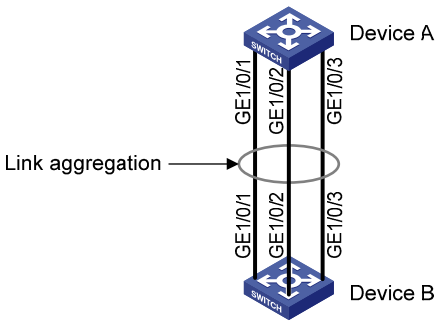
## Layer 2 Static Aggregation Configuration Example

### Network requirements

As shown in Figure 1-1, Device A and Device B are connected through their respective Ethernet ports GigabitEthernet1/0/1 to GigabitEthernet1/0/3.

Aggregate the ports on each device to form a static link aggregation group, thus balancing outgoing traffic across the member ports. In addition, perform load sharing based on source and destination MAC addresses.

**Figure 1-1** Network diagram for Layer 2 static aggregation




### Configuration procedure

1) Configure Device A

# Configure the device to perform load sharing based on source and destination MAC addresses for link aggregation groups.

```
<DeviceA> system-view
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac
```

# Create Layer 2 aggregate interface Bridge-aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

# Assign Layer 2 Ethernet interfaces GigabitEthernet1/0/1 through GigabitEthernet1/0/3 to aggregation group 1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface GigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
```

2) Configure Device B

Follow the same configuration procedure performed on Device A to configure Device B.

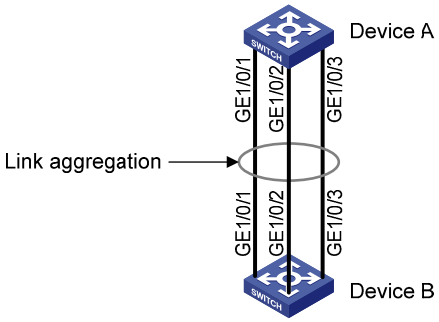
# Layer 2 Dynamic Aggregation Configuration Example

## Network requirements

As shown in Figure 1-2, Device A and Device B are connected through their respective Ethernet ports GigabitEthernet1/0/1 to GigabitEthernet1/0/3.

Aggregate the ports on each device to form a dynamic link aggregation group, thus balancing outgoing traffic across the member ports. In addition, perform load sharing based on source and destination MAC addresses.

**Figure 1-2** Network diagram for Layer 2 dynamic aggregation




## Configuration procedure

1) Configure Device A

# Configure the device to perform load sharing based on source and destination MAC addresses for link aggregation groups.

```
<DeviceA> system-view
[DeviceA] link-aggregation load-sharing mode source-mac destination-mac
```

# Create a Layer 2 aggregate interface Bridge-Aggregation 1 and configure the interface to work in dynamic aggregation mode.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

# Assign Layer 2 Ethernet interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA- GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface GigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
```

2) Configure Device B

Follow the same configuration procedure performed on Device A to configure Device B.

# Table of Contents

# 1 Port Isolation Configuration

When configuring port isolation, go to these sections for information you are interested in:



## Introduction to Port Isolation

Usually, Layer 2 traffic isolation is achieved by assigning ports to different VLANs. To save VLAN resources, port isolation is introduced to isolate ports within a VLAN, allowing for great flexibility and security.

Currently:

- Some devices support only one isolation group that is created automatically by the system as isolation group 1. These devices are referred to as single-isolation-group devices. You can neither remove the isolation group nor create other isolation groups on such devices.
- There is no restriction on the number of ports assigned to an isolation group.

## Configuring the Isolation Group for a Single-Isolation-Group Device

### Assigning a Port to the Isolation Group

Follow these steps to add a port to the isolation group:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or, port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use one of the commands.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports.<br>• In port group view, the subsequent configurations apply to all ports in the port group. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Assign the port or ports to the isolation group as an isolated port or ports | | **port-isolate enable** | Required<br>No ports are added to the isolation group by default. |

# Displaying and Maintaining Isolation Groups

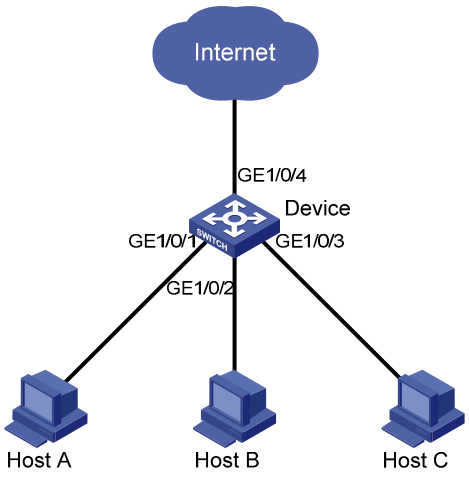
| To do… | Use the command… | Remarks |
|---|---|---|
| Display the isolation group information on a single-isolation-group device | **display port-isolate group** | Available in any view |

# Port Isolation Configuration Example

## Network requirements

- Users Host A, Host B, and Host C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of Device.
- Device is connected to the Internet through GigabitEthernet 1/0/4.
- GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet1/0/3 and GigabitEthernet1/0/4 belong to the same VLAN. It is desired that Host A, Host B, and Host C cannot communicate with one another at Layer 2, but can access the Internet.

**Figure 1-1** Networking diagram for port isolation configuration




## Configuration procedure

# Add ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to the isolation group.

```
<Device> system-view
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface GigabitEthernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface GigabitEthernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable
```

# Display the information about the isolation group.

```
<Device> display port-isolate group
```

```
Port-isolate group information:
Uplink port support: NO
Group ID: 1
Group members:
  GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
```

# Table of Contents

# 1 DLDP Configuration

When performing DLDP configuration, go to these sections for information you are interested in:



## Overview

Sometimes, unidirectional links may appear in networks. On a unidirectional link, one end can receive packets from the other end but the other end cannot. Unidirectional links result in problems such as loops in an STP-enabled network.

As for fiber links, two kinds of unidirectional links exist. One occurs when fibers are cross-connected, as shown in Figure 1-1. The other occurs when one end of a fiber is not connected or one fiber of a fiber pair gets disconnected, as illustrated by the hollow arrows in Figure 1-2.

**Figure 1-1** Unidirectional fiber link: cross-connected fibers

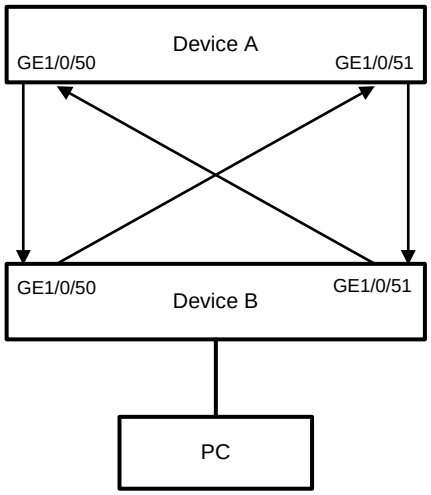
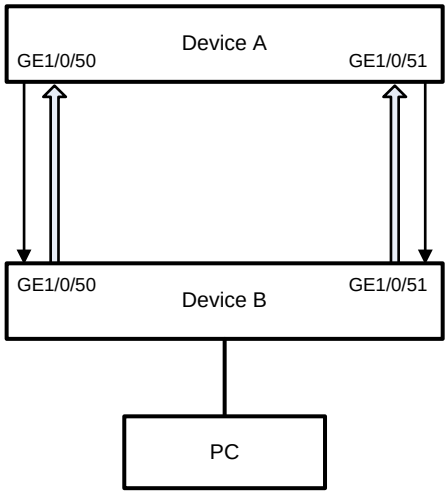


**Figure 1-2** Unidirectional fiber link: a fiber not connected or disconnected




## DLDP Introduction

Device Link Detection Protocol (DLDP) can detect the link status of a fiber cable or twisted pair. On detecting a unidirectional link, DLDP can shut down the related port automatically or prompt users to take measures as configured to avoid network problems.

As a data link layer protocol, DLDP cooperates with physical layer protocols to monitor the link status of a device. While the auto-negotiation mechanism provided by the physical layer detects physical signals and faults, DLDP performs operations such as identifying peer devices, detecting unidirectional links, and shutting down unreachable ports. The cooperation of physical layer protocols and DLDP ensures that physical/logical unidirectional links be detected and shut down. For a link with the devices on the both sides of it operating properly, DLDP checks to see if the cable is connected correctly and if packets can be exchanged between the two devices. Note that DLDP is not implemented through auto-negotiation.

## DLDP Fundamentals

### DLDP link states

A device is in one of these DLDP link states: Initial, Inactive, Active, Advertisement, Probe, Disable, and DelayDown, as described in Table 1-1.

**Table 1-1** DLDP link states

| State | Indicates… |
|---|---|
| Initial | DLDP is disabled. |
| Inactive | DLDP is enabled but the link is down. |
| Active | DLDP is enabled and the link is up, or the neighbor entries have been cleared. |
| Advertisement | All neighbors are bi-directionally reachable or DLDP has been in active state for more than five seconds. This is a relatively state where no unidirectional link has been detected. |
| Probe | DLDP enters this state if it receives a packet from an unknown neighbor. In this state, DLDP sends packets to check whether the link is unidirectional. As soon as DLDP transits to this state, a probe timer starts and an echo timeout timer starts for each neighbor to be probed. |

| State | Indicates… |
|---|---|
| Disable | A port enters this state when:<br>• A unidirectional link is detected.<br>• The contact with the neighbor in enhanced mode gets lost.<br>In this state, the port does not receive or send packets other than DLDPDUs. |
| DelayDown | A port in the Active, Advertisement, or Probe DLDP link state transits to this state rather than removes the corresponding neighbor entry and transits to the Inactive state when it detects a port-down event. When a port transits to this state, the DelayDown timer is triggered. |

## DLDP timers

**Table 1-2** DLDP timers

| DLDP timer | Description |
|---|---|
| Active timer | Determines the Interval for sending Advertisement packets with RSY tags, which defaults to 1 second. That is, a device in the active DLDP link state sends one Advertisement packet with RSY tags every second by default. The maximum number of advertisement packets with RSY tags that can be sent successively is 5. |
| Advertisement timer | Determines the interval to send advertisement packets, which defaults to 5 seconds. |
| Probe timer | Determines the interval to send Probe packets, which defaults to 0.5 seconds. That is, a device in the probe state sends two Probe packets every second by default. The maximum number of Probe packets that can be sent successively is 10. |
| Echo timer | This timer is set to 10 seconds and is triggered when a device transits to the Probe state or an enhanced detect is launched. When the Echo timer expires and no Echo packet has been received from a neighbor device, the state of the link is set to unidirectional and the device transits to the Disable state. In this case, the device sends Disable packets, prompts the user to shut down the port or shuts down the port automatically (depending on the DLDP down mode configured), and removes the corresponding neighbor entries. |
| Entry timer | When a new neighbor joins, a neighbor entry is created and the corresponding entry timer is triggered. When a DLDP packet is received, the device updates the corresponding neighbor entry and the entry aging timer.<br>In the normal mode, if no packet is received from a neighbor when the corresponding entry aging timer expires, DLDP sends advertisement packets with RSY tags and removes the neighbor entry.<br>In the enhanced mode, if no packet is received from a neighbor when the Entry timer expires, DLDP triggers the enhanced timer.<br>The setting of an Entry timer is three times that of the Advertisement timer. |
| Enhanced timer | In the enhanced mode, this timer is triggered if no packet is received from a neighbor when the entry aging timer expires. Enhanced timer is set to 1 second.<br>After the Enhanced timer is triggered, the device sends up to eight probe packets to the neighbor at a frequency of one packet per second. |

| DLDP timer | Description |
|---|---|
| DelayDown timer | A device in the Active, Advertisement, or Probe DLDP link state transits to DelayDown state rather than removes the corresponding neighbor entry and transits to the Inactive state when it detects a port-down event.<br>When a device transits to this state, the DelayDown timer is triggered. A device in DelayDown state only responds to port-up events.<br>A device in the DelayDown state resumes its original DLDP state if it detects a port-up event before the DelayDown timer expires. Otherwise, it removes the corresponding DLDP neighbor information and transits to the Inactive state. |
| RecoverProbe timer | This timer is set to 2 seconds. That is, a port in the Disable state sends one RecoverProbe packet every two seconds to detect whether a unidirectional link has restored. |

## DLDP mode

DLDP can operate in two modes: normal mode and enhanced mode, as described below.

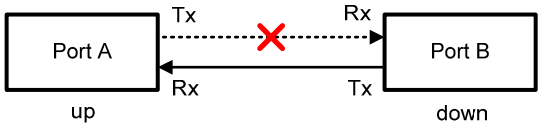
- In normal DLDP mode, when an entry timer expires, the device removes the corresponding neighbor entry and sends an Advertisement packet with RSY tag.
- In enhanced DLDP mode, when an entry timer expires, the Enhanced timer is triggered and the device sends up to eight Probe packets at a frequency of one packet per second to test the neighbor. If no Echo packet is received from the neighbor when the Echo timer expires, the device transits to the Disable state.

**Table 1-3** DLDP mode and neighbor entry aging

| DLDP mode | Detecting a neighbor after the corresponding neighbor entry ages out | Removing the neighbor entry immediately after the Entry timer expires | Triggering the Enhanced timer after an Entry timer expires |
|---|---|---|---|
| Normal DLDP mode | No | Yes | No |
| Enhanced DLDP mode | Yes | No | Yes |

The enhanced DLDP mode is designed for addressing black holes. It prevents the cases where one end of a link is up and the other is down. If you configure the speed and the duplex mode by force on a device, the situation shown in Figure 1-3 may occur, where Port B is actually down but the state of Port B cannot be detected by common data link protocols, so Port A is still up. In enhanced DLDP mode, however, Port A tests Port B after the Entry timer concerning Port B expires. Port A then transits to the Disable state if it receives no Echo packet from Port A when the Echo timer expires. As Port B is physically down, it is in the Inactive DLDP state.

**Figure 1-3** A case for Enhanced DLDP mode




**Note**

- In normal DLDP mode, only fiber cross-connected unidirectional links (as shown in Figure 1-1 ) can be detected.
- In enhanced DLDP mode, two types of unidirectional links can be detected. One is fiber cross-connected links (as shown in Figure 1-1). The other refers to fiber pairs with one fiber not connected or disconnected (as shown in Figure 1-2). To detect unidirectional links that are of the latter type, you need to configure the ports to operate at specific speed and in full duplex mode. Otherwise, DLDP cannot take effect. When a fiber of a fiber pair is not connected or gets disconnected, the port that can receive optical signals is in Disable state; the other port is in Inactive state.

## DLDP authentication mode

You can prevent network attacks and illegal detect through DLDP authentication. Three DLDP authentication modes exist, as described below.

- Non-authentication. In this mode, the sending side sets the Authentication field and the Authentication type field of DLDP packets to 0. The receiving side checks the values of the two fields of received DLDP packets and drops the packets with the two fields conflicting with the corresponding local configuration.
- Plain text authentication. In this mode, before sending a DLDP packet, the sending side sets the Authentication field to the password configured in plain text and sets the Authentication type field to 1. The receiving side checks the values of the two fields of received DLDP packets and drops the packets with the two fields conflicting with the corresponding local configuration.
- MD5 authentication. In this mode, before sending a packet, the sending side encrypts the user configured password using MD5 algorithm, assigns the digest to the Authentication field, and sets the Authentication type field to 2. The receiving side checks the values of the two fields of received DLDP packets and drops the packets with the two fields conflicting with the corresponding local configuration.

## DLDP implementation

1) On a DLDP-enabled link that is in up state, DLDP sends DLDP packets to the peer device and processes the DLDP packets received from the peer device. DLDP packets sent vary with DLDP states. Table 1-4 lists DLDP states and the corresponding packets.

**Table 1-4** DLDP packet types and DLDP states

| DLDP state | Type of DLDP packets sent |
|---|---|
| Active | Advertisement packet with RSY tag |
| Advertisement | Normal Advertisement packet |
| Probe | Probe packet |
| Disable | Disable packet and RecoverProbe packet |

**Note**

When a device transits from a DLDP state other than Inactive state or Disable state to Initial state, it sends Flush packets.

2) A received DLDP packet is processed as follows.

- In any of the three authentication modes, the packet is dropped if it fails to pass the authentication.
- The packet is dropped if the setting of the interval for sending Advertisement packets it carries conflicts with the corresponding local setting.
- Other processes.

**Table 1-5** Procedures for processing different types of DLDP packets

| Packet type | Processing procedure | |
|---|---|---|
| Advertisement packet with RSY tag | Retrieving the neighbor information. | If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state. |
| | | If the corresponding neighbor entry already exists, resets the Entry timer and transits to Probe state. |
| Normal Advertisement packet | Retrieves the neighbor information. | If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state. |
| | | If the corresponding neighbor entry already exists, resets the Entry timer. |
| Flush packet | Determines whether or not the local port is in Disable state. | If yes, no process is performed. |
| | | If not, removes the corresponding neighbor entry (if any). |
| Probe packet | Retrieves the neighbor information. | If the corresponding neighbor entry does not exist, creates the neighbor entry, transits to Probe state, and returns Echo packets. |
| | | If the corresponding neighbor entry already exists, resets the Entry timer and returns Echo packets. |

<table>
<tr><th>Packet type</th><th colspan="3">Processing procedure</th></tr>
<tr><td rowspan="3">Echo packet</td><td rowspan="3">Retrieves the neighbor information.</td><td colspan="2">If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.</td></tr>
<tr><td rowspan="2">The corresponding neighbor entry already exists</td><td>If the neighbor information it carries conflicts with the corresponding locally maintained neighbor entry, drops the packet.</td></tr>
<tr><td>Otherwise, sets the flag of the neighbor as two-way connected. In addition, if the flags of all the neighbors are two-way connected, the device transits from Probe state to Advertisement state and disables the Echo timer.</td></tr>
<tr><td rowspan="2">Disable packet</td><td rowspan="2">Check to see if the local port is in Disable state.</td><td colspan="2">If yes, no process is performed.</td></tr>
<tr><td colspan="2">If not, the local port transits to Disable state.</td></tr>
<tr><td rowspan="2">RecoverProbe packet</td><td rowspan="2">Check to see if the local port is in Disable or Advertisement state.</td><td colspan="2">If not, no process is performed.</td></tr>
<tr><td colspan="2">If yes, returns RecoverEcho packets.</td></tr>
<tr><td rowspan="2">RecoverEcho packet</td><td rowspan="2">Check to see if the local port is in Disable state.</td><td colspan="2">If not, no process is performed.</td></tr>
<tr><td colspan="2">If yes, the local port transits to Active state if the neighbor information the packet carries is consistent with the local port information.</td></tr>
<tr><td rowspan="2">LinkDown packet</td><td rowspan="2">Check to see if the local port operates in Enhanced mode.</td><td colspan="2">If not, no process is performed.</td></tr>
<tr><td colspan="2">If yes and the local port is not in Disable state, the local transits to Disable state.</td></tr>
</table>

3) If no echo packet is received from the neighbor, DLDP performs the following processing.

**Table 1-6** Processing procedure when no echo packet is received from the neighbor

| No echo packet received from the neighbor | Processing procedure |
|---|---|
| In normal mode, no echo packet is received when the Echo timer expires. | DLDP transits to the Disable state, outputs log and tracking information, and sends Disable packets. In addition, depending on the user-defined DLDP down mode, DLDP shuts down the local port or prompts users to shut down the port, and removes the corresponding neighbor entry. |
| In enhanced mode, no echo packet is received when the enhanced timer expires. | |

### Link auto-recovery mechanism

If the port shutdown mode upon detection of a unidirectional link is set to **auto**, DLDP sets the state of the port where a unidirectional link is detected to DLDP down automatically. A DLDP down port cannot forward service traffic or send/receive any PDUs except DLDPDUs.

On a DLDP down port, DLDP monitors the unidirectional link. Once DLDP finds out that the state of the link has restored to bidirectional, it brings up the port. The specific process is as follows:

The DLDP down port sends out a RecoverProbe packet, which carries only information about the local port, every two seconds. Upon receiving the RecoverProbe packet, the remote end returns a RecoverEcho packet. Upon receiving the RecoverEcho packet, the local port checks whether neighbor information in the RecoverEcho packet is the same as the local port information. If they are the same, the link between the local port and the neighbor is considered to have been restored to a bidirectional link, and the port will transit from Disable state to Active state and re-establish neighborship with the neighbor.

Only DLDP down ports can send and process Recover packets, including RecoverProbe packets and RecoverEcho packets. The auto-recovery mechanism does not take effect on ports manually shut down.

### DLDP neighbor state

A DLDP neighbor can be in one of the three states described in Table 1-7.

**Table 1-7** Description on DLDP neighbor states

| DLDP neighbor state | Description |
|---|---|
| Unknown | A neighbor is in this state when it is just detected and is being probed. No information indicating the state of the neighbor is received. A neighbor is in this state only when it is being probed. It transits to Two way state or Unidirectional state after the probe operation finishes. |
| Two way | A neighbor is in this state after it receives response from its peer. This state indicates the link is a two-way link. |
| Unidirectional | A neighbor is in this state when the link connecting it is detected to be a unidirectional link. After a device transits to this state, the corresponding neighbor entries maintained on other devices are removed. |

## DLDP Configuration Task List

Complete the following tasks to configure DLDP:

| Task | Remarks |
|---|---|
| Enabling DLDP | Required |
| Setting DLDP Mode | Optional |
| Setting the Interval for Sending Advertisement Packets | Optional |
| Setting the DelayDown Timer | Optional |
| Setting the Port Shutdown Mode | Optional |
| Configuring DLDP Authentication | Optional |
| Resetting DLDP State | Optional |

Note that:

- DLDP takes effects only on Ethernet interfaces.
- DLDP can detect unidirectional links only after all links are connected. Therefore, before enabling DLDP, make sure that optical fibers or copper twisted pairs are connected.

- To ensure unidirectional links can be detected, make sure these settings are the same on the both sides: DLDP state (enabled/disabled), the interval for sending Advertisement packets, authentication mode, and password.
- Keep the interval for sending Advertisement packets adequate to enable unidirectional links to be detected in time. If the interval is too long, unidirectional links cannot be terminated in time; if the interval is too short, network traffic may increase in vain.
- DLDP does not process any link aggregation control protocol (LACP) events. The links in an aggregation group are treated individually in DLDP.
- When connecting two DLDP-enabled devices, make sure the DLDP software version ID fields of the DLDP packets exchanged between the two devices are the same. Otherwise, DLDP may operate improperly.

## Enabling DLDP

Follow these steps to enable DLDP:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable DLDP globally | | **dldp enable** | Required<br>Globally disabled by default |
| Enter Ethernet port view or port group view | Enter Ethernet port view | **interface** *interface-type interface-number* | Either of the two is required.<br>The configuration performed in Ethernet port view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable DLDP | | **dldp enable** | Required<br>Disabled on a port by default<br>You can perform this operation on an optical port or an electrical port. |

**Caution**

DLDP takes effect only when it is enabled both globally and on a port.

## Setting DLDP Mode

Follow these steps to set DLDP mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set DLDP mode | **dldp work-mode** { **enhance** \| **normal** } | Optional<br>Normal by default |

## Setting the Interval for Sending Advertisement Packets

You can set the interval for sending Advertisement packets to enable unidirectional links to be detected in time.

Follow these steps to set the interval for sending Advertisement packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the interval for sending Advertisement packets | **dldp interval** *time* | Optional<br>5 seconds by default<br>The interval for sending Advertisement packets applies to all the DLDP-enabled ports. |

**Caution**

- Set the interval for sending Advertisement packets to a value not longer than one-third of the STP convergence time. If the interval is too long, STP loops may occur before unidirectional links are torn down, and it takes a long time for the device to detect unidirectional links, thus causing more traffic forwarding errors; if the interval is too short, unnecessary Advertisement packets can be generated to consume bandwidth. Therefore, you are recommended to use the default value.
- To enable DLDP to operate properly, make sure the intervals for sending Advertisement packets on both sides of a link are the same.

## Setting the DelayDown Timer

On some ports, when the Tx line fails, the port goes down and then comes up again, causing optical signal jitters on the Rx line. When a port goes down due to a Tx failure, the device transits to the DelayDown state instead of the Inactive state to prevent the corresponding neighbor entries from being removed. In the same time, the device triggers the DelayDown timer. If the port goes up before the timer expires, the device restores the original state; if the port remains down when the timer expires, the devices transits to the Inactive state.

Follow these steps to set the DelayDown timer

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the DelayDown timer | **dldp delaydown-timer** *time* | Optional<br>1 second by default<br>DelayDown timer setting applies to all the DLDP-enabled ports. |

## Setting the Port Shutdown Mode

On detecting a unidirectional link, the ports can be shut down in one of the following two modes.

- Manual mode. This mode applies to networks with low performance, where normal links may be treated as unidirectional links. It protects service packet transmission against false unidirectional links. In this mode, DLDP only detects unidirectional links and generates log and traps. The operations to shut down unidirectional link ports are accomplished by the administrator.
- Auto mode. In this mode, when a unidirectional link is detected, DLDP transits to Disable state, generates log and traps, and set the port as DLDP Down.

Follow these steps to set port shutdown mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set port shutdown mode | **dldp unidirectional-shutdown** { **auto** \| **manual** } | Optional<br>**auto** by default |

**Caution**

- On a port with both remote OAM loopback and DLDP enabled, if the port shutdown mode is auto mode, the port will be shut down by DLDP when it receives a packet sent by itself, causing remote OAM loopback to operate improperly. To prevent this, you need to set the port shutdown mode to auto mode.
- If the device is busy, or the CPU utilization is high, normal links may be treated as unidirectional links. In this case, you can set the port shutdown mode to manual mode to eliminate the effects caused by false unidirectional link report.

## Configuring DLDP Authentication

Follow these steps to configure DLDP authentication:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure DLDP authentication | **dldp authentication-mode** { **md5** *md5-password* \| **none** \| **simple** *simple-password* } | Required<br>**none** by default |

**Caution**

To enable DLDP to operate properly, make sure the DLDP authentication modes and the passwords of the both sides of a link are the same.

## Resetting DLDP State

After DLDP detects a unidirectional link on a port, the port enters Disable state. In this case, DLDP prompts you to shut down the port manually or shuts down the port automatically depending on the

user-defined port shutdown mode. To enable the port to perform DLDP detect again, you can reset the DLDP state of the port in one of the following methods:

- If the port is shut down with the **shutdown** command manually, use the **undo shutdown** command on the port.
- If the port is shut down by DLDP automatically, use the **dldp reset** command on the port. Alternatively, you can leave the work to DLDP, which can enable the port automatically upon detecting that the link has been restored to bidirectional. For how to reset DLDP state with the **dldp reset** command, refer to Resetting DLDP State in System View and Resetting DLDP State in Port view/Port Group View.

The DLDP state that the port transits to upon the DLDP state reset operation depends on its physical state. If the port is physically down, it transits to Inactive state; if the port is physically up, it transits to Active state.

### Resetting DLDP State in System View

Resetting DLDP state in system view applies to all the ports shut down by DLDP.

Follow these steps to reset DLDP in system view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Reset DLDP state | **dldp reset** | Required |

### Resetting DLDP State in Port view/Port Group View

Resetting DLDP state in port view or port group view applies to the current port or all the ports in the port group shut down by DLDP.

Follow these steps to reset DLDP state in port view/port group view:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet port view/port group view | Enter Ethernet port view | **interface** *interface-type interface-number* | Either is required.<br>The configuration performed in Ethernet port view applies to the current port only; the configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Reset DLDP state | | **dldp reset** | Required |

## Displaying and Maintaining DLDP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the DLDP configuration of a port | **display dldp** [ *interface-type interface-number* ] | Available in any view |
| Display the statistics on DLDP packets passing through a port | **display dldp statistics** [ *interface-type interface-number* ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear the statistics on DLDP packets passing through a port | **reset dldp statistics** [ *interface-type interface-number* ] | Available in user view |

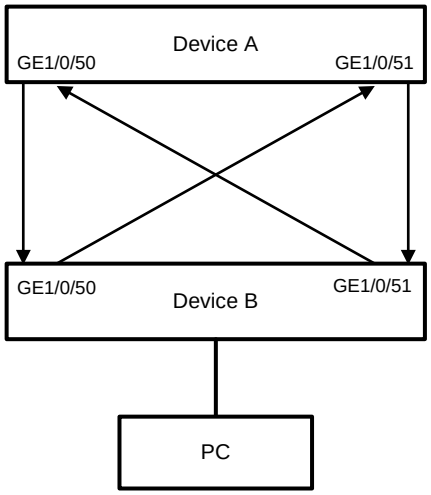
# DLDP Configuration Example

## DLDP Configuration Example

### Network requirements

- Device A and Device B are connected through two fiber pairs, in which two fibers are cross-connected, as shown in Figure 1-4.
- It is desired that the unidirectional links can be disconnected on being detected; and the ports shut down by DLDP can be restored after the fiber connections are corrected.

**Figure 1-4** Network diagram for DLDP configuration




### Configuration procedure

1) Configuration on Device A

# Enable DLDP on GigabitEthernet1/0/50 and GigabitEthernet 1/0/51.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
[DeviceA] interface gigabitethernet 1/0/51
[DeviceA-GigabitEthernet1/0/51] dldp enable
[DeviceA-GigabitEthernet1/0/51] quit
```

# Set the interval for sending Advertisement packets to 6 seconds.

```
[DeviceA] dldp interval 6
```

# Set the DelayDown timer to 2 seconds.

```
[DeviceA] dldp delaydown-timer 2
```

# Set the DLDP mode as enhanced mode.

```
[DeviceA] dldp work-mode enhance
```

# Set the port shutdown mode as auto mode.

```
[DeviceA] dldp unidirectional-shutdown auto
```

# Enable DLDP globally.

```
[DeviceA] dldp enable
```

# Check the information about DLDP.

```
[DeviceA] display dldp
DLDP global status : enable
DLDP interval : 6s
DLDP work-mode : enhance
DLDP authentication-mode  : none
DLDP unidirectional-shutdown : auto
DLDP delaydown-timer : 2s
The number of enabled ports is 2.

Interface GigabitEthernet1/0/50
DLDP port state : disable
DLDP link state : down
The neighbor number of the port is 0.

Interface GigabitEthernet1/0/51
DLDP port state : disable
DLDP link state : down
The neighbor number of the port is 0.
```

The output information indicates that both GigabitEthernet 1/0/50 and GigabitEthernet 1/0/51 are in Disable state and the links are down, which means unidirectional links are detected and the two ports are thus shut down.

# Reset DLDP state for the ports shut down by DLDP.

```
[DeviceA] dldp reset
```

2) Configuration on Device B

The configuration on Device B is the same as that on Device A and is thus omitted.

---

**Note**

If two fibers are cross-connected, all the four ports involved will be shut down by DLDP.

---

## Troubleshooting

**Symptom:**

Two DLDP-enabled devices, Device A and Device B, are connected through two fiber pairs, in which two fibers are cross-connected. The unidirectional links cannot be detected; all the four ports involved are in Advertisement state.

**Analysis:**

The problem can be caused by the following.

- The intervals for sending Advertisement packets on Device A and Device B are not the same.
- DLDP authentication modes/passwords on Device A and Device B are not the same.

**Solution:**

Make sure the interval for sending Advertisement packets, the authentication mode, and the password on Device A and Device B are the same.

# Table of Contents

# 1 LLDP Configuration

When configuring LLDP, go to these sections for information you are interested in:



## Introduction to LLDP

### Overview

The Link Layer Discovery Protocol (LLDP) operates on the data link layer. It stores and maintains information about the local device and the devices directly connected to it for network administrators to manage networks through NMS (network management systems). In LLDP, device information is encapsulated in LLDPDUs in the form of TLV (meaning type, length, and value) triplets and is exchanged between directly connected devices. Information in LLDPDUs received is stored in standard MIB (management information base).

### LLDP Fundamental

#### LLDP operating mode

LLDP can operate in one of the following modes.

- TxRx mode. A port in this mode sends and receives LLDPDUs.
- Tx mode. A port in this mode only sends LLDPDUs.
- Rx mode. A port in this mode only receives LLDPDUs.
- Disable mode. A port in this mode does not send or receive LLDPDUs.

LLDP is initialized when an LLDP-enabled port changes to operate in another LLDP operating mode. To prevent LLDP from being initialized too frequently, LLDP undergoes a period before being initialized on an LLDP-enabled port when the port changes to operate in another LLDP operating mode. The period is known as initialization delay, which is determined by the re-initialization delay timer.

#### Sending LLDPDUs

An LLDP-enabled device operating in TxRx mode or Tx mode sends LLDPDUs to its directly connected devices periodically. It also sends LLDPDUs when the local configuration changes to inform the neighboring devices of the change timely. In any of the two cases, an interval exists between two successive operations of sending LLDPDUs. This prevents the network from being overwhelmed by LLDPDUs even if the LLDP operating mode changes frequently.

To enable the neighboring devices to be informed of the existence of a device or an LLDP operating mode change (from the disable mode to TxRx mode, or from the Rx mode to Tx mode) timely, a device can invoke the fast sending mechanism. In this case, the interval to send LLDPDUs changes to one second. After the device sends specific number of LLDPDUs, the interval restores to the normal. (A neighbor is discovered when a device receives an LLDPDU and no information about the sender is locally available.)

### Receiving LLDPDUs

An LLDP-enabled device operating in TxRx mode or Rx mode checks the TLVs carried in the LLDPDUs it receives and saves the valid neighboring information. An LLDPDU also carries a TTL (time to live) setting with it. The information about a neighboring device maintained locally ages out when the corresponding TTL expires.

The TTL of the information about a neighboring device is determined by the following expression:

TTL multiplier × LLDPDU sending interval

You can set the TTL by configuring the TTL multiplier. Note that the TTL can be up to 65535 seconds. TTLs longer than it will be rounded off to 65535 seconds.

## TLV Types

TLVs encapsulated in LLDPDUs fall into these categories: basic TLV, organization defined TLV, and MED (media endpoint discovery) related TLV. Basic TLVs are the base of device management. Organization specific TLVs and MED related TLVs are used for enhanced device management. They are defined in standards or by organizations and are optional to LLDPDUs.

### Basic LLDP TLVs

Table 1-1 lists the basic LLDP TLV types that are currently in use.

**Table 1-1** Basic LLDP TLVs

| Type | Description | Remarks |
|---|---|---|
| End of LLDPDU TLV | Marks the end of an LLDPDU. | Required for LLDP |
| Chassis ID TLV | Carries the bridge MAC address of the sender | |
| Port ID TLV | Carries the sending port. For devices that do not send MED TLVs, port ID TLVs carry sending port name. For devices that send MED TLVs, port ID TLVs carry the MAC addresses of the sending ports or bridge MAC addresses (if the MAC addresses of the sending ports are unavailable). | |
| Time To Live TLV | Carries the TTL of device information | |

| Type | Description | Remarks |
|---|---|---|
| Port Description TLV | Carries Ethernet port description | Optional to LLDP |
| System Name TLV | Carries device name | |
| System Description TLV | Carries system description | |
| System Capabilities TLV | Carries information about system capabilities | |
| Management Address TLV | Carries the management address, the corresponding port number, and OID (object identifier).<br>If the management address is not configured, it is the IP address of the interface of the VLAN with the least VLAN ID among those permitted on the port. If the IP address of the VLAN interface is not configured, IP address 127.0.0.1 is used as the management address. | |

### Organization defined LLDP TLVs

1) LLDP TLVs defined in IEEE802.1 include the following:

- Port VLAN ID TLV, which carries port VLAN ID.
- Port and protocol VLAN ID TLV, which carries port protocol VLAN ID.
- VLAN name TLV, which carries port VLAN name.
- Protocol identity TLV, which carries types of the supported protocols.

**Note**

Currently, protocol identity TLVs can only be received on the 3Com Switch 4500G.

2) IEEE 802.3 defined LLDP TLVs include the following:

- MAC/PHY configuration/status TLV, which carries port configuration, such as port speed, duplex state, whether port speed auto-negotiation is supported, the state of auto-negotiation, current speed , and current duplex state.
- Power via MDI TLV, which carries information about power supply capabilities.
- Link aggregation TLV, which carries the capability and state of link aggregation.
- Maximum frame size TLV, which carries the maximum frame size supported, namely, MTU (maximum transmission unit).

### MED related LLDP TLVs

LLDP-MED TLVs provide multiple advanced applications for VoIP, such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs satisfy the voice device manufacturers' requirements for cost-effectiveness, easy deployment, and easy management. In addition, LLDP-MED TLVs make deploying voice devices in Ethernet easier.

- LLDP-MED capabilities TLV, which carries the MED type of the current device and the types of the LLDP MED TLVs that can be encapsulated in LLDPDUs.
- Network policy TLV, which carries port VLAN ID, supported applications (such as voice and video services), application priority, and the policy adopted.

- Extended power-via-MDI TLV, which carries the information about the power supply capability of the current device.
- Hardware revision TLV, which carries the hardware version of an MED device.
- Firmware revision TLV, which carries the firmware version of an MED device.
- Software revision TLV, which carries the software version of an MED device.
- Serial number TLV, which carries the serial number of an MED device.
- Manufacturer name TLV, which carries the manufacturer name of an MED device.
- Model name TLV, which carries the model of an MED device.
- Asset ID TLV, which carries the asset ID of an MED device. Asset ID is used for directory management and asset tracking.
- Location identification TLV, which carries the location identification of a device. Location identification can be used in location-based applications.

**Note**

For detailed information about LLDP TLV, refer to *IEEE 802.1AB-2005* and *ANSI/TIA-1057*.

### Protocols and Standards

- IEEE 802.1AB-2005, Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057, Link Layer Discovery Protocol for Media Endpoint Devices

## LLDP Configuration Task List

Complete these tasks to configure LLDP:

| Task | | Remarks |
|---|---|---|
| Basic LLDP configuration | Enabling LLDP | Required |
| | Setting LLDP Operating Mode | Optional |
| | Configuring LLDPDU TLVs | Optional |
| | Enable LLDP Polling | Optional |
| | Configuring the Parameters Concerning LLDPDU Sending | Optional |
| Configuring the Encapsulation Format for LLDPDUs | | Optional |
| Configuring the Encapsulation Format of the Management Address | | Optional |
| Configuring CDP Compatibility | | Optional |
| Configuring LLDP Trapping | | Optional |

## Performing Basic LLDP Configuration

### Enabling LLDP

Follow these steps to enable LLDP:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable LLDP globally | | **lldp enable** | Required<br>By default, LLDP is enabled globally. |
| Enter Ethernet interface view/port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable LLDP | | **lldp enable** | Optional<br>By default, LLDP is enabled on a port. |

**Note**

To make LLDP take effect, you need to enable it both globally and on the related ports.

## Setting LLDP Operating Mode

Follow these steps to set LLDP operating mode:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Set the initialization delay period | | **lldp timer reinit-delay** *value* | Optional<br>2 seconds by default. |
| Enter Ethernet interface view/port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Set the LLDP operating mode | | **lldp admin-status** { **disable** \| **rx** \| **tx** \| **txrx** } | Optional<br>TxRx by default. |

## Configuring LLDPDU TLVs

Follow these steps to configure LLDPDU TLVs:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Set the TTL multiplier | | **lldp hold-multiplier** *value* | Optional<br>4 by default. |
| Enter Ethernet interface view/port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable LLDP TLV sending for specific types of LLDP TLVs | | **lldp tlv-enable** { **basic-tlv** { **all** \| **port-description** \| **system-capability** \| **system-description** \| **system-name** } \| **dot1-tlv** { **all** \| **port-vlan-id** \| **protocol-vlan-id** [ *vlan-id* ] \| **vlan-name** [ *vlan-id* ] } \| **dot3-tlv** { **all** \| **link-aggregation** \| **mac-physic** \| **max-frame-size** \| **power** } \| **med-tlv** { **all** \| **capability** \| **inventory** \| **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }*&<1–10>* \| **elin-address** *tel-number* } \| **network-policy** \| **power-over-ethernet** } } | Optional<br>By default, all types of LLDP TLVs except location identification TLV are sent. |
| Specify the management address and specify to send the management address through LLDPDUs | | **lldp management-address-tlv** [ *ip-address* ] | Optional<br>By default, the management address is sent through LLDPDUs, and the management address is the IP address of the interface of the VLAN with the least VLAN ID among those permitted on the port. If the IP address of the VLAN interface is not configured, IP address 127.0.0.1 is used as the management address. Refer to *VLAN Configuration* in the *Access Volume* for information about VLAN. |

**Note**

- To enable MED related LLDP TLV sending, you need to enable LLDP-MED capabilities TLV sending first. Conversely, to disable LLDP-MED capabilities TLV sending, you need to disable the sending of other MED related LLDP TLVs.
- To disable MAC/PHY configuration/status TLV sending, you need to disable LLDP-MED capabilities TLV sending first.
- When executing the **lldp tlv-enable** command, specifying the **all** keyword for basic LLDP TLVs and organization defined LLDP TLVs (including IEEE 802.1 defined LLDP TLVs and IEEE 802.3 defined LLDP TLVs) enables sending of all the corresponding LLDP TLVs. For MED related LLDP TLVs, the **all** keyword enables sending of all the MED related LLDP TLVs except location identification TLVs.
- Enabling sending of LLDP-MED capabilities TLVs also enables sending of MAC/PHY configuration/status TLVs.

## Enable LLDP Polling

With LLDP polling enabled, a device checks for the local configuration changes periodically. Upon detecting a configuration change, the device sends LLDPDUs to inform the neighboring devices of the change.

Follow these steps to enable LLDP polling:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view/port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable LLDP polling and set the polling interval | | **lldp check-change-interval** *value* | Required<br>Disabled by default |

## Configuring the Parameters Concerning LLDPDU Sending

### Configuring time-related parameters

Follow these steps to set time-related parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **System-view** | — |
| Set the interval to send LLDPDUs | **lldp timer tx-interval** *value* | Optional<br>30 seconds by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the delay period to send LLDPDUs | **lldp timer tx-delay** *value* | Optional<br>2 seconds by default |

**Caution**

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

### Setting the number of the LLDPDUs to be sent when a new neighboring device is detected

Follow these steps to set the number of the LLDPDUs to be sent when a new neighboring device is detected

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the number of the LLDPDUs to be sent successively when a new neighboring device is detected | **lldp fast-count** *value* | Optional<br>3 by default |

## Configuring the Encapsulation Format for LLDPDUs

LLDPDUs can be encapsulated in Ethernet II or SNAP frames.

- With Ethernet II encapsulation configured, an LLDP port sends LLDPDUs in Ethernet II frames and processes only Ethernet II encapsulated incoming LLDPDUs.
- With SNAP encapsulation configured, an LLDP port sends LLDPDUs in SNAP frames and processes only SNAP encapsulated incoming LLDPDUs.

By default, LLDPDUs are encapsulated in Ethernet II frames. If the neighbor devices encapsulate LLDPDUs in SNAP frames, you can configure the encapsulation format for LLDPDUs as SNAP, thus guaranteeing communication with the other devices in the network.

Follow these steps to configure the encapsulation format for LLDPDUs:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the encapsulation format for LLDPDUs as SNAP | | **lldp encapsulation snap** | Required<br>Ethernet II encapsulation format applies by default. |

**Note**

The configuration does not apply to LLDP-CDP packets, which use only SNAP encapsulation.

## Configuring the Encapsulation Format of the Management Address

LLDP encapsulates the management address in the form of numbers or strings in management address TLVs and then advertises it.

By default, management addresses are encapsulated in the form of numbers in TLVs. If neighbors encapsulate management addresses in the form of strings in TLVs, you can configure the encapsulation format of the management address as strings, thus guaranteeing communication with the other devices in the network.

Follow these steps to configure the encapsulation format of the management address:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the encapsulation format of the management address as strings in TLVs | | lldp management-address-format string | Required<br>By default, the management address is encapsulated in the form of numbers in TLVs. |

## Configuring CDP Compatibility

**Note**

For detailed information about voice VLAN, refer to *VLAN Configuration* in the *Access Volume*.

You need to enable CDP compatibility for your device to work with Cisco IP phones.

As your LLDP-enabled device cannot recognize CDP packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. This can cause a requesting Cisco IP phone to send voice traffic without any tag to your device, disabling your device to differentiate the voice traffic from other types of traffic.

By configuring CDP compatibility, you can enable LLDP on your device to receive and recognize CDP packets from Cisco IP phones and respond with CDP packets carrying the voice VLAN configuration

TLV for the IP phones to configure the voice VLAN automatically. Thus, the voice traffic is confined in the configured voice VLAN to be differentiated from other types of traffic.

CDP-compatible LLDP operates in one of the follows two modes:

- TxRx where CDP packets can be transmitted and received.
- Disable where CDP packets can neither be transmitted nor be received.

### Configuration Prerequisites

Before configuring CDP compatibility, make sure that:

- LLDP is enabled globally.
- LLDP is enabled on the port connected to an IP phone and is configured to operate in TxRx mode on the port.

### Configuring CDP Compatibility

Follow these steps to enable LLDP to be compatible with CDP:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable CDP compatibility globally | | **lldp compliance cdp** | Required<br>Disabled by default. |
| Enter Ethernet interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure CDP-compatible LLDP to operate in TxRx mode | | **lldp compliance admin-status cdp txrx** | Required<br>By default, CDP-compatible LLDP operates in disable mode. |

**Caution**

As the maximum TTL allowed by CDP is 255 seconds, your TTL configuration, that is, the product of the TTL multiplier and the LLDPDU sending interval, must be less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.

## Configuring LLDP Trapping

LLDP trapping is used to notify NMS of the events such as new neighboring devices detected and link malfunctions.

LLDP traps are sent periodically and you can set the interval to send LLDP traps. In response to topology changes detected, a device sends LLDP traps according to the interval configured to inform the neighboring devices of the changes.

Follow these steps to configure LLDP trap:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view/port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Either of the two is required.<br>Configuration performed in Ethernet interface view applies to the current port only; configuration performed in port group view applies to all the ports in the corresponding port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable LLDP trap sending | | **lldp notification remote-change enable** | Required<br>Disabled by default |
| Quit to system view | | **quit** | — |
| Set the interval to send LLDP traps | | **lldp timer notification-interval** *value* | Optional<br>5 seconds by default |

# Displaying and Maintaining LLDP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the global LLDP information or the information contained in the LLDP TLVs to be sent through a port | **display lldp local-information** [ **global** \| **interface** *interface-type interface-number* ] | Available in any view |
| Display the information contained in the LLDP TLVs received through a port | **display lldp neighbor-information** [ **interface** *interface-type interface-number* ] [ **brief** ] | Available in any view |
| Display LLDP statistics | **display lldp statistics** [ **global** \| **interface** *interface-type interface-number* ] | Available in any view |
| Display LLDP status of a port | **display lldp status** [ **interface** *interface-type interface-number* ] | Available in any view |
| Display the types of the LLDP TLVs that are currently sent | **display lldp tlv-config** [ **interface** *interface-type interface-number* ] | Available in any view |

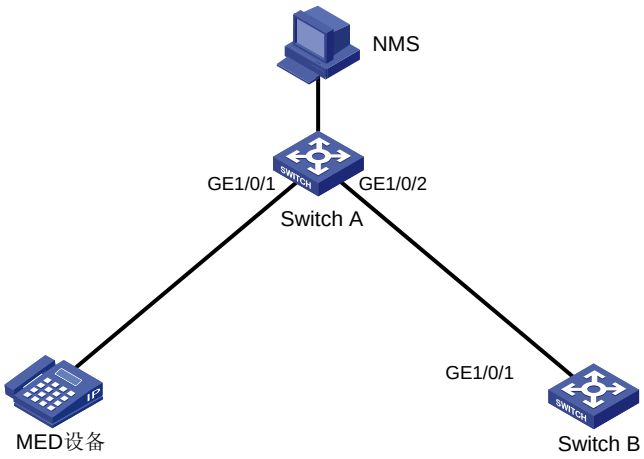
# LLDP Configuration Examples

## LLDP Basic Configuration Example

### Network requirements

- The NMS and Switch A are located in the same Ethernet. An MED device and Switch B are connected to GigabitEthernet1/0/1 and GigabitEthernet1/0/2 of Switch A.
- Enable LLDP on the ports of Switch A and Switch B to monitor the link between Switch A and Switch B and the link between Switch A and the MED device on the NMS.

**Figure 1-1** Network diagram for LLDP configuration




## Configuration procedure

1) Configure Switch A.

# Enable LLDP globally.

```
<SwitchA> system-view
[SwitchA] lldp enable
```

# Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, setting the LLDP operating mode to Rx.

```
[SwitchA] interface gigabitethernet1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

2) Configure Switch B.

# Enable LLDP globally.

```
<SwitchB> system-view
[SwitchB] lldp enable
```

# Enable LLDP on GigabitEthernet1/0/1, setting the LLDP operating mode to Tx.

```
[SwitchB] interface gigabitethernet1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

3) Verify the configuration.

# Display the global LLDP status and port LLDP status on Switch A.

```
[SwitchA] display lldp status
Global status of LLDP : Enable
The current number of LLDP neighbors : 2
The current number of CDP neighbors : 0
LLDP neighbor information last changed time : 0 days, 0 hours, 4 minutes, 40 seconds
```

```
Transmit interval              : 30s
Hold multiplier                : 4
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3

Port 1 [GigabitEthernet1/0/1] :
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Roll time                      : 0s

Number of neighbors             : 1
Number of MED neighbors         : 1
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV  : 0

Port 2 [GigabitEthernet1/0/2] :
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
Roll time                      : 0s

Number of neighbors             : 1
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV  : 3
```

# Tear down the link between Switch A and Switch B and then display the global LLDP status and port LLDP status on Switch A.

```
[SwitchA] display lldp status
Global status of LLDP : Enable
The current number of LLDP neighbors : 1
The current number of CDP neighbors : 0
LLDP neighbor information last changed time : 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Hold multiplier                : 4
Reinit delay                   : 2s
Transmit delay                 : 2s
Trap interval                  : 5s
Fast start times               : 3

Port 1 [GigabitEthernet1/0/1] :
Port status of LLDP            : Enable
Admin status                   : Rx_Only
```

```
Trap flag                       : No
Roll time                       : 0s

Number of neighbors              : 1
Number of MED neighbors          : 1
Number of CDP neighbors          : 0
Number of sent optional TLV      : 0
Number of received unknown TLV   : 5

Port 2 [GigabitEthernet1/0/2] :
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
Roll time                       : 0s

Number of neighbors              : 0
Number of MED neighbors          : 0
Number of CDP neighbors          : 0
Number of sent optional TLV      : 0
Number of received unknown TLV   : 0
```

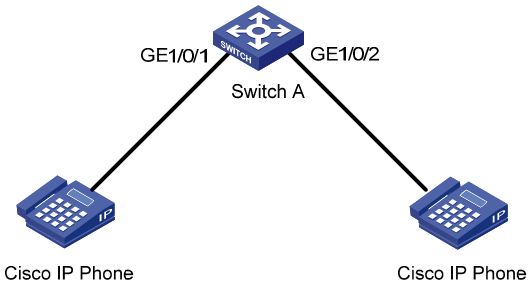
## CDP-Compatible LLDP Configuration Example

### Network requirements

- GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone.
- Configure voice VLAN 2 on Switch A. Enable CDP compatibility of LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN, thus confining their voice traffic within the voice VLAN to be isolated from other types of traffic.

### Network diagram

**Figure 1-2** Network diagram for LLDP compatible with CDP configuration




### Configuration procedure

1) Configure the voice VLAN on Switch A

# Create VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

# Configure the link type of the ports to be trunk and enable the voice VLAN feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/2] quit
```

2) Configure CDP-compatible LLDP on Switch A.

# Enable LLDP globally.

```
[SwitchA] lldp enable
```

# Enable LLDP to be compatible with CDP globally.

```
[SwitchA] lldp compliance cdp
```

# Enable LLDP, configure LLDP to operate in TxRx mode, and configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

3) Verify the configuration

# Display the neighbor information on Switch A.

```
[SwitchA] display lldp neighbor-information
CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  CDP neighbor index : 1
  Chassis ID         : SEP00141CBCDBFE
  Port ID            : Port 1
  Sofrware version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex             : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  CDP neighbor index : 2
  Chassis ID         : SEP00141CBCDBFF
  Port ID            : Port 1
  Sofrware version   : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex             : Full
```

# Table of Contents

# 1 MSTP Configuration

When configuring MSTP, go to these sections for information you are interested in:



## MSTP Overview

### Introduction to STP

#### Why STP?

The Spanning Tree Protocol (STP) was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging information with one another and eliminate loops by selectively blocking certain ports to prune the loop structure into a loop-free tree structure. This avoids proliferation and infinite cycling of packets that would occur in a loop network and prevents decreased performance of network devices caused by duplicate packets received.

In the narrow sense, STP refers to IEEE 802.1d STP; in the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

#### Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP-enabled network devices exchange BPDUs to establish a spanning tree. BPDUs contain sufficient information for the network devices to complete spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used for calculating a spanning tree and maintaining the spanning tree topology.
- Topology change notification (TCN) BPDUs, used for notifying the concerned devices of network topology changes, if any.

#### Basic concepts in STP

1) Root bridge

A tree network must have a root; hence the concept of root bridge was introduced in STP.

There is one and only one root bridge in the entire network, and the root bridge can change along with changes of the network topology. Therefore, the root bridge is not fixed.

After network convergence, the root bridge generates and sends out configuration BPDUs at a certain interval, and other devices just forward the BPDUs. This mechanism ensures stable topologies.

2) Root port

On a non-root bridge, the port nearest to the root bridge is called the root port. The root port is responsible for communication with the root bridge. Each non-root bridge has one and only one root port. The root bridge has no root port.

3) Designated bridge and designated port

The following table describes designated bridges and designated ports.

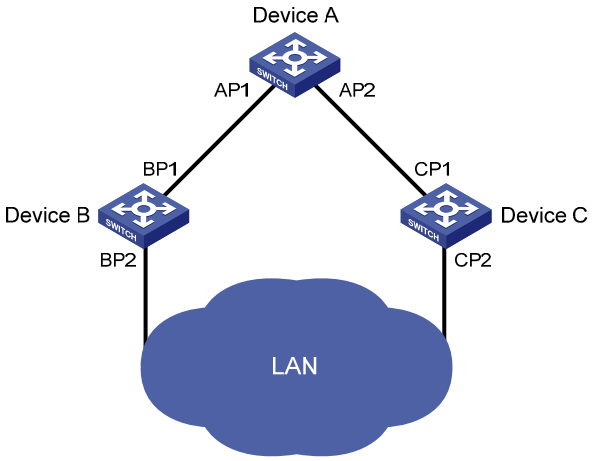
**Table 1-1** Description of designated bridges and designated ports:

| Classification | Designated bridge | Designated port |
|---|---|---|
| For a device | A device directly connected with the local device and responsible for forwarding BPDUs to the local device | The port through which the designated bridge forwards BPDUs to this device |
| For a LAN | The device responsible for forwarding BPDUs to this LAN segment | The port through which the designated bridge forwards BPDUs to this LAN segment |

As shown in Figure 1-1, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port of Device B is port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port for the LAN is the port BP2 on Device B.

**Figure 1-1** A schematic diagram of designated bridges and designated ports



**Note**

All the ports on the root bridge are designated ports.

4) Path cost

Path cost is a reference value used for link selection in STP. By calculating path costs, STP selects relatively robust links and blocks redundant links, and finally prunes the network into a loop-free tree.

### How STP works

The devices on a network exchange BPDUs to identify the network topology. Configuration BPDUs contain sufficient information for the network devices to complete spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID: consisting of the priority and MAC address of the root bridge.
- Root path cost: the cost of the path to the root bridge.
- Designated bridge ID: consisting of the priority and MAC address of the designated bridge.
- Designated port ID: designated port priority plus port name.
- Message age: age of the configuration BPDU while it propagates in the network.
- Max age: maximum age of the configuration BPDU.
- Hello time: configuration BPDU transmission interval.
- Forward delay: the delay used by STP bridges to transit the state of the root and designated ports to forwarding.

**Note**

For simplicity, the descriptions and examples below involve only four fields of configuration BPDUs:

- Root bridge ID (represented by device priority)
- Root path cost (related to the rate of the link connected to the port)
- Designated bridge ID (represented by device priority)
- Designated port ID (represented by port name)

### Calculation process of the STP algorithm

1) Initial state

Upon initialization of a device, each port generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

2) Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

**Table 1-2** Selection of the optimum configuration BPDU

| Step | Actions |
|---|---|
| 1 | Upon receiving a configuration BPDU on a port, the device performs the following:<br>• If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device discards the received configuration BPDU and does not process the configuration BPDU of this port.<br>• If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device replaces the content of the configuration BPDU generated by the port with the content of the received configuration BPDU. |
| 2 | The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU. |

**Note**

The following are the principles of configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all the configuration BPDUs have the same root bridge ID, their root path costs are compared. Assume that the root path cost in a configuration BPDU plus the path cost of a receiving port is S. The configuration BPDU with the smallest S value has the highest priority.
- If all configuration BPDUs have the same ports value, their designated bridge IDs, designated port IDs, and the IDs of the receiving ports are compared in sequence. The configuration BPDU containing a smaller ID wins out.

3) Selection of the root bridge

Initially, each STP-enabled device on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the devices compare their root bridge IDs to elect the device with the smallest root bridge ID as the root bridge.

4) Selection of the root port and designated ports on a non-root device

The process of selecting the root port and designated ports is as follows:

**Table 1-3** Selection of the root port and designated ports

| Step | Description |
|---|---|
| 1 | A non-root-bridge device regards the port on which it received the optimum configuration BPDU as the root port. |
| 2 | Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports.<br>• The root bridge ID is replaced with that of the configuration BPDU of the root port.<br>• The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost of the root port.<br>• The designated bridge ID is replaced with the ID of this device.<br>• The designated port ID is replaced with the ID of this port. |

| Step | Description |
|---|---|
| 3 | The device compares the calculated configuration BPDU with the configuration BPDU on the port of which the port role is to be defined, and acts depending on the comparison result:<br>• If the calculated configuration BPDU is superior, the device considers this port as the designated port, and replaces the configuration BPDU on the port with the calculated configuration BPDU, which will be sent out periodically.<br>• If the configuration BPDU on the port is superior, the device blocks this port without updating its configuration BPDU. The blocked port can receive BPDUs but not send BPDUs or forward data. |

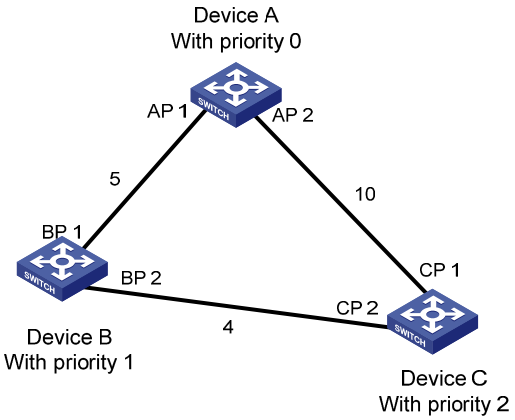
**Note**

When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state – they receive BPDUs but do not forward BPDUs or user traffic.

A tree-shape topology forms upon successful election of the root bridge, the root port on each non-root bridge and the designated ports.

The following is an example of how the STP algorithm works. As shown in Figure 1-2, assume that the priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

**Figure 1-2** Network diagram for the STP algorithm




- Initial state of each device

The following table shows the initial state of each device.

**Table 1-4** Initial state of each device

| Device | Port name | BPDU of port |
|---|---|---|
| Device A | AP1 | {0, 0, 0, AP1} |
| | AP2 | {0, 0, 0, AP2} |
| Device B | BP1 | {1, 0, 1, BP1} |
| | BP2 | {1, 0, 1, BP2} |

| Device | Port name | BPDU of port |
|---|---|---|
| Device C | CP1 | {2, 0, 2, CP1} |
| | CP2 | {2, 0, 2, CP2} |

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

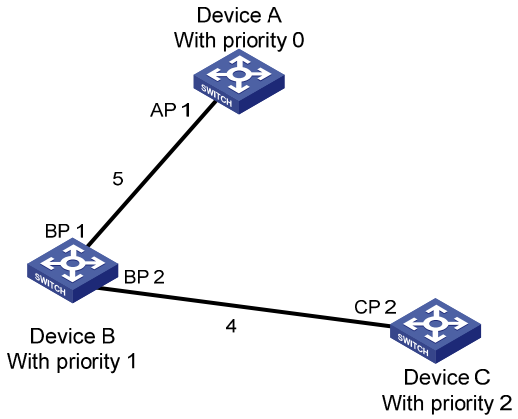
**Table 1-5** Comparison process and result on each device

| Device | Comparison process | BPDU of port after comparison |
|---|---|---|
| Device A | • Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU.<br>• Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU.<br>• Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically. | AP1: {0, 0, 0, AP1}<br>AP2: {0, 0, 0, AP2} |
| Device B | • Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1.<br>• Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU. | BP1: {0, 0, 0, AP1}<br>BP2: {1, 0, 1, BP2} |
| | • Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed.<br>• Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}.<br>• Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. As the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically. | Root port BP1:<br>{0, 0, 0, AP1}<br>Designated port BP2:<br>{0, 5, 1, BP2} |

| Device | Comparison process | BPDU of port after comparison |
|---|---|---|
| Device C | • Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1.<br>• Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the configuration BPDU is updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and therefore updates the configuration BPDU of CP2. | CP1: {0, 0, 0, AP2}<br>CP2: {1, 0, 1, BP2} |
| | After comparison:<br>• The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed.<br>• Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU. | Root port CP1:<br>{0, 0, 0, AP2}<br>Designated port CP2:<br>{0, 10, 2, CP2} |
| | • Then, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its own configuration BPDU, Device C launches a BPDU update process.<br>• At the same time, port CP1 receives periodic configuration BPDUs from Device A. Device C does not launch an update process after comparison. | CP1: {0, 0, 0, AP2}<br>CP2: {0, 5, 1, BP2} |
| | After comparison:<br>• Because the root path cost of CP2 (9) (root path cost of the BPDU (5) plus path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed.<br>• After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new event, for example, the link from Device B to Device C going down. | Blocked port CP2:<br>{0, 0, 0, AP2}<br>Root port CP2:<br>{0, 5, 1, BP2} |

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is established as shown in Figure 1-3.

**Figure 1-3** The final calculated spanning tree




**Note**

The spanning tree calculation process in this example is only simplified process.

## The BPDU forwarding mechanism in STP

- Upon network initiation, every switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular hello interval.
- If it is the root port that received a configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device increases the message age carried in the configuration BPDU following a certain rule and starts a timer to time the configuration BPDU while sending out this configuration BPDU through the designated port.
- If the configuration BPDU received on a designated port has a lower priority than the configuration BPDU of the local port, the port immediately sends out its own configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device will generate a configuration BPDU with itself as the root and send out the BPDUs and TCN BPDUs. This triggers a new spanning tree calculation process to establish a new path to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root ports and designated ports begin to forward data as soon as they are elected, a temporary loop may occur.

## STP timers

STP calculation involves three important timing parameters: forward delay, hello time, and max age.

- Forward delay is the delay time for device state transition.

A path failure can cause spanning tree re-calculation to adapt the spanning tree structure to the change. However, the resulting new configuration BPDU cannot propagate throughout the network immediately. If the newly elected root ports and designated ports start to forward data right away, a temporary loop is likely to occur.

For this reason, as a mechanism for state transition in STP, the newly elected root ports or designated ports require twice the forward delay time before transiting to the forwarding state to ensure that the new configuration BPDU has propagated throughout the network.

- Hello time is the time interval at which a device sends hello packets to the surrounding devices to ensure that the paths are fault-free.
- Max age is a parameter used to determine whether a configuration BPDU held by the device has expired. A configuration BPDU beyond the max age will be discarded.

## Introduction to MSTP

### Why MSTP

1) Weakness of STP and RSTP

STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or an edge port, which directly connects to a user terminal rather than to another device or a shared LAN segment.

The Rapid Spanning Tree Protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to converge.

---

**Note**

- In RSTP, a newly elected root port can enter the forwarding state rapidly if this condition is met: The old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.
- In RSTP, a newly elected designated port can enter the forwarding state rapidly if this condition is met: The designated port is an edge port or a port connected with a point-to-point link. If the designated port is an edge port, it can enter the forwarding state directly; if the designated port is connected with a point-to-point link, it can enter the forwarding state immediately after the device undergoes handshake with the downstream device and gets a response.

---

Although RSTP supports rapid network convergence, it has the same drawback as STP does: All bridges within a LAN share the same spanning tree, so redundant links cannot be blocked based on VLAN, and the packets of all VLANs are forwarded along the same spanning tree.

2) Features of MSTP

The Multiple Spanning Tree Protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to the support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along separate paths, thus providing a better load sharing mechanism for redundant links. For description about VLANs, refer to *VLAN Configuration* in the *Access Volume*.

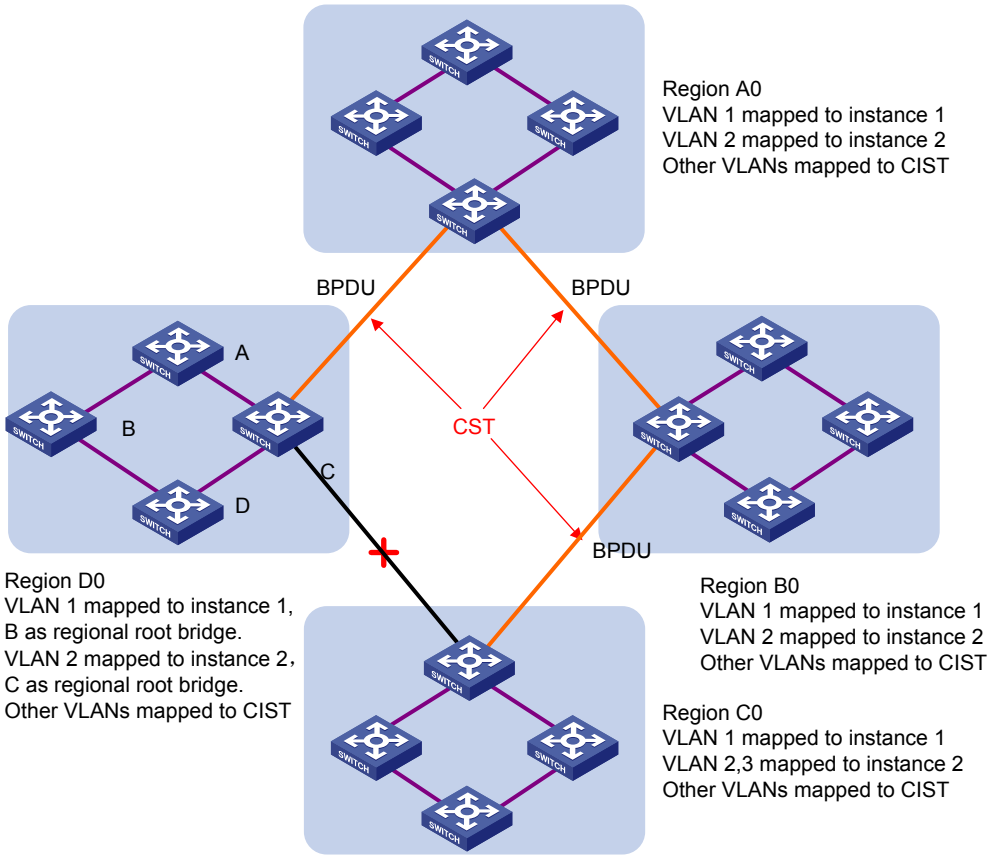
MSTP features the following:

- MSTP supports mapping VLANs to MST instances (MSTIs) by means of a VLAN-to-MSTI mapping table. MSTP can reduce communication overheads and resource usage by mapping multiple VLANs to one MSTI.

- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a loop network into a loop-free tree, thus avoiding proliferation and endless cycling of packets in a loop network. In addition, it provides multiple redundant paths for data forwarding, thus supporting load balancing of VLAN data.
- MSTP is compatible with STP and RSTP.

## Basic concepts in MSTP

**Figure 1-4** Basic concepts in MSTP




Assume that all devices in Figure 1-4 are running MSTP. This section explains some basic concepts of MSTP.

2) MST region

A multiple spanning tree region (MST region) consists of multiple devices in a switched network and the network segments among them. These devices have the following characteristics:

- All are MSTP-enabled,
- They have the same region name,
- They have the same VLAN-to-MSTI mapping configuration,
- They have the same MSTP revision level configuration, and
- They are physically linked with one another.

For example, all the devices in region A0 in Figure 1-4 have the same MST region configuration:

- The same region name,
- The same VLAN-to-MSTI mapping configuration (VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to the common and internal spanning tree (CIST, that is, MSTI 0), and
- The same MSTP revision level (not shown in the figure).

Multiple MST regions can exist in a switched network. You can use an MSTP command to assign multiple devices to the same MST region.

3) VLAN-to-MSTI mapping table

As an attribute of an MST region, the VLAN-to-MSTI mapping table describes the mapping relationships between VLANs and MSTIs. In Figure 1-4, for example, the VLAN-to-MSTI mapping table of region A0 is as follows: VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to CIST. MSTP achieves load balancing by means of the VLAN-to-MSTI mapping table.

4) IST

An internal spanning tree (IST) is a spanning tree that runs in an MST region.

ISTs in all MST regions and the common spanning tree (CST) jointly constitute the common and internal spanning tree (CIST) of the entire network. An IST is a section of the CIST.

In Figure 1-4, for example, the CIST has a section in each MST region, and this section is the IST in the respective MST region.

5) CST

The CST is a single spanning tree that connects all MST regions in a switched network. If you regard each MST region as a “device”, the CST is a spanning tree calculated by these “devices” through STP or RSTP. For example, the red lines in Figure 1-4 represent the CST.

6) CIST

Jointly constituted by ISTs and the CST, the CIST is a single spanning tree that connects all devices in a switched network.

In Figure 1-4, for example, the ISTs in all MST regions plus the inter-region CST constitute the CIST of the entire network.

7) MSTI

Multiple spanning trees can be generated in an MST region through MSTP, one spanning tree being independent of another. Each spanning tree is referred to as a multiple spanning tree instance (MSTI). In Figure 1-4, for example, multiple spanning trees can exist in each MST region, each spanning tree corresponding to the specific VLAN(s). These spanning trees are called MSTIs.

8) Regional root bridge

The root bridge of the IST or an MSTI within an MST region is the regional root bridge of the IST or the MSTI. Based on the topology, different spanning trees in an MST region may have different regional roots.

For example, in region D0 in Figure 1-4, the regional root of MSTI 1 is device B, while that of MSTI 2 is device C.

9) Common root bridge

The common root bridge is the root bridge of the CIST.

In Figure 1-4, for example, the common root bridge is a device in region A0.

10) Boundary port

A boundary port is a port that connects an MST region to another MST region, or to a single spanning-tree region running STP, or to a single spanning-tree region running RSTP. In Figure 1-4, for example, if a device in region A0 is interconnected with the first port of a device in region D0 and the common root bridge of the entire switched network is located in region A0, the first port of that device in region D0 is the boundary port of region D0.

During MSTP calculation, a boundary port's role on an MSTI is consistent with its role on the CIST. But that is not true with master ports. A master port on MSTIs is a root port on the CIST.

11) Roles of ports

MSTP calculation involves these port roles: root port, designated port, master port, alternate port, backup port, and so on.

- Root port: a port responsible for forwarding data to the root bridge.
- Designated port: a port responsible for forwarding data to the downstream network segment or device.
- Master port: A port on the shortest path from the current region to the common root bridge, connecting the MST region to the common root bridge. If the region is seen as a node, the master port is the root port of the region on the CST. The master port is a root port on IST/CIST and still a master port on the other MSTIs.
- Alternate port: The standby port for the root port and the master port. When the root port or master port is blocked, the alternate port becomes the new root port or master port.
- Backup port: The backup port of a designated port. When the designated port is blocked, the backup port becomes a new designated port and starts forwarding data without delay. A loop occurs when two ports of the same MSTP device are interconnected. Therefore, the device will block either of the two ports, and the backup port is that port to be blocked.

A port can play different roles in different MSTIs.

**Figure 1-5** Port roles

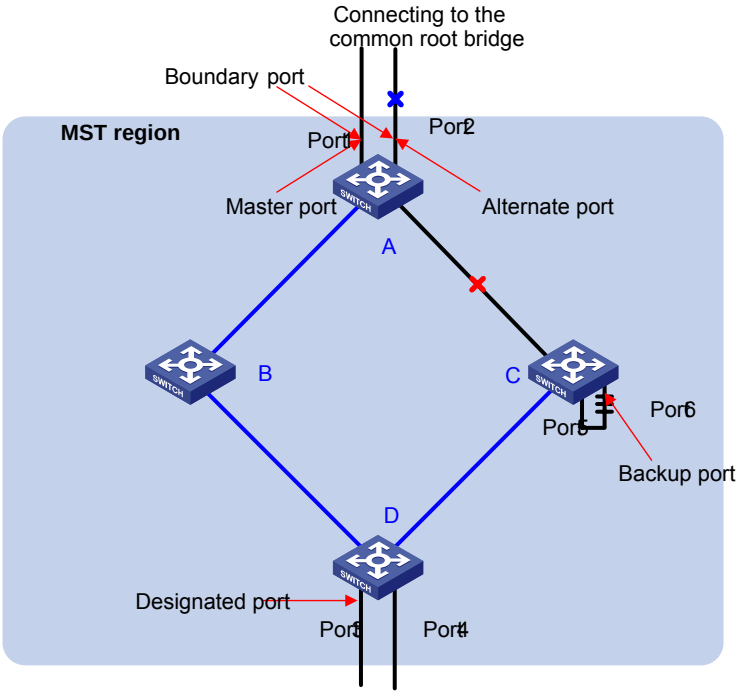



Figure 1-5 helps understand these concepts. In this figure:

- Devices A, B, C, and D constitute an MST region.
- Port 1 and port 2 of device A connect to the common root bridge.
- Port 5 and port 6 of device C form a loop.
- Port 3 and port 4 of device D connect downstream to other MST regions.

12) Port states

In MSTP, port states fall into the following three:

- Forwarding: the port learns MAC addresses and forwards user traffic;
- Learning: the port learns MAC addresses but does not forward user traffic;
- Discarding: the port neither learns MAC addresses nor forwards user traffic.

---

**Note**

When in different MSTIs, a port can be in different states.

---

A port state is not exclusively associated with a port role. Table 1-6 lists the port state(s) supported by each port role ("√" indicates that the port supports this state, while "—" indicates that the port does not support this state).

**Table 1-6** Ports states supported by different port roles

| Port role (right) / Port state (below) | Root port/master port | Designated port | Alternate port | Backup port |
|---|---|---|---|---|
| Forwarding | √ | √ | — | — |
| Learning | √ | √ | — | — |
| Discarding | √ | √ | √ | √ |

## How MSTP works

MSTP divides an entire Layer 2 network into multiple MST regions, which are interconnected by a calculated CST. Inside an MST region, multiple spanning trees are calculated, each being called an MSTI. Among these MSTIs, MSTI 0 is the IST, while all the others are MSTIs. Similar to STP, MSTP uses configuration BPDUs to calculate spanning trees. The only difference between the two protocols is that an MSTP BPDU carries the MSTP configuration on the device from which this BPDU is sent.

1) CIST calculation

The calculation of a CIST tree is also the process of configuration BPDU comparison. During this process, the device with the highest priority is elected as the root bridge of the CIST. MSTP generates an IST within each MST region through calculation, and, at the same time, MSTP regards each MST region as a single device and generates a CST among these MST regions through calculation. The CST and ISTs constitute the CIST of the entire network.

2) MSTI calculation

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-MSTI mappings. MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP, for each spanning tree. For details, refer to How STP works.

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

### Implementation of MSTP on devices

MSTP is compatible with STP and RSTP. STP and RSTP protocol packets can be recognized by devices running MSTP and used for spanning tree calculation.

In addition to basic MSTP functions, many special functions are provided for ease of management, as follows:

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU guard

## Protocols and Standards

MSTP is documented in:

- IEEE 802.1d: Spanning Tree Protocol
- IEEE 802.1w: Rapid Spanning Tree Protocol
- IEEE 802.1s: Multiple Spanning Tree Protocol

# Configuration Task List

Before configuring MSTP, you need to know the position of each device in each MSTI: root bridge or leave node. In each MSTI, one, and only one device acts as the root bridge, while all others as leaf nodes.

Complete these tasks to configure MSTP:

| Task | | Remarks |
|---|---|---|
| Configuring the Root Bridge | Configuring an MST Region | Required |
| | Specifying the Root Bridge or a Secondary Root Bridge | Optional |
| | Configuring the Work Mode of an MSTP Device | Optional |
| | Configuring the Priority of the Current Device | Optional |
| | Configuring the Maximum Hops of an MST Region | Optional |
| | Configuring the Network Diameter of a Switched Network | Optional |
| | Configuring Timers of MSTP | Optional |
| | Configuring the Timeout Factor | Optional |
| | Configuring the Maximum Port Rate | Optional |
| | Configuring Ports as Edge Ports | Optional |
| | Setting the Link Type of a Port to P2P | Optional |
| | Configuring the Mode a Port Uses to Recognize/Send MSTP Packets | Optional |
| | Enabling the Output of Port State Transition Information | Optional |
| | Enabling the MSTP Feature | Required |

| Task | | Remarks |
|---|---|---|
| Configuring Leaf NodesConfiguring Leaf Nodes | Configuring an MST Region | Required |
| | Configuring the Work Mode of an MSTP Device | Optional |
| | Configuring the Timeout Factor | Optional |
| | Configuring the Maximum Port Rate | Optional |
| | Configuring Ports as Edge Ports | Optional |
| | Configuring Path Costs of Ports | Optional |
| | Configuring Port Priority | Optional |
| | Setting the Link Type of a Port to P2P | Optional |
| | Configuring the Mode a Port Uses to Recognize/Send MSTP Packets | Optional |
| | Enabling the Output of Port State Transition Information | Optional |
| | Enabling the MSTP Feature | Required |
| Performing mCheck | | Optional |
| Configuring Digest Snooping | | Optional |
| Configuring No Agreement Check | | Optional |
| Configuring Protection Functions | | Optional |

**Note**

- If both GVRP and MSTP are enabled on a device at the same time, GVRP packets will be forwarded along the CIST. Therefore, if you wish to advertise a certain VLAN within the network through GVRP in this case, make sure that this VLAN is mapped to the CIST (MSTI 0) when configuring the VLAN-to-MSTI mapping table. For the detailed information of GVRP, refer to *GVRP Configuration* of the *Access Volume*.
- MSTP is mutually exclusive with any of the following functions on a port: service loopback, RRPP, Smart Link, and BPDU tunnel.
- Configurations made in Layer-2 aggregate interface view can take effect only on the aggregate interface; configurations made on an aggregation member port can take effect only after the port is removed from the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- After you enable MSTP on a Layer-2 aggregate interface, the system performs MSTP calculation on the Layer-2 aggregate interface but not on the aggregation member ports. The MSTP enable state and forwarding state of each selected port in an aggregation group is consistent with those of the corresponding Layer-2 aggregate interface.
- Though the member port of an aggregation group does not participate in MSTP calculation, the port still reserves its MSTP configurations for participating MSTP calculation after leaving the aggregation group.

# Configuring the Root Bridge

## Configuring an MST Region

### Configuration procedure

Follow these steps to configure an MST region:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MST region view | **stp region-configuration** | — |
| Configure the MST region name | **region-name** *name* | Optional<br>The MST region name is the MAC address by default. |
| Configure the VLAN-to-MSTI mapping table | **instance** *instance-id* **vlan** *vlan-list* | Optional<br>Use either command.<br>All VLANs in an MST region are mapped to MSTI 0 by default. |
| | **vlan-mapping modulo** *modulo* | |
| Configure the MSTP revision level of the MST region | **revision-level** *level* | Optional<br>0 by default |
| Activate MST region configuration manually | **active region-configuration** | Required |
| Display all the configuration information of the MST region | **check region-configuration** | Optional |
| Display the currently effective MST region configuration information | **display stp region-configuration** | The **display** command can be executed in any view. |

**Note**

Two or more MSTP-enabled devices belong to the same MST region only if they are configured to have the same MST region name, the same VLAN-to-MSTI mapping entries in the MST region and the same MST region revision level, and they are interconnected via a physical link.

The configuration of MST region–related parameters, especially the VLAN-to-MSTI mapping table, will cause MSTP to launch a new spanning tree calculation process, which may result in network topology instability. To reduce the possibility of topology instability caused by configuration, MSTP will not immediately launch a new spanning tree calculation process when processing MST region–related configurations; instead, such configurations will take effect only after you:

- activate the MST region–related parameters using the **active region-configuration** command, or
- enable MSTP using the **stp enable** command.

### Configuration example

# Configure the MST region name to be “info”, the MSTP revision level to be 1, and VLAN 2 through VLAN 10 to be mapped to MSTI 1 and VLAN 20 through VLAN 30 to MSTI 2.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name info
[Sysname-mst-region] instance 1 vlan 2 to 10
[Sysname-mst-region] instance 2 vlan 20 to 30
[Sysname-mst-region] revision-level 1
[Sysname-mst-region] active region-configuration
```

## Specifying the Root Bridge or a Secondary Root Bridge

MSTP can determine the root bridge of a spanning tree through MSTP calculation. Alternatively, you can specify the current device as the root bridge using the commands provided by the system.

### Specifying the current device as the root bridge of a specific spanning tree

Follow these steps to specify the current device as the root bridge of a specific spanning tree:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify the current device as the root bridge of a specific spanning tree | **stp** [ **instance** *instance-id* ] **root primary** | Required<br>By default, a device does not function as the root bridge. |

### Specifying the current device as a secondary root bridge of a specific spanning tree

Follow these steps to specify the current device as a secondary root bridge of a specific spanning tree:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify the current device as a secondary root bridge of a specific spanning tree | **stp** [ **instance** *instance-id* ] **root secondary** | Required<br>By default, a device does not function as a secondary root bridge. |

Note that:

- After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.
- You can configure the current device as the root bridge or a secondary root bridge of an MSTI, which is specified by **instance** *instance-id* in the command. If you set *instance-id* to 0, the current device will be the root bridge or a secondary root bridge of the CIST.
- The current device has independent roles in different MSTIs. It can act as the root bridge or a secondary root bridge of one instance while it can also act as the root bridge or a secondary root bridge of another MSTI. However, the same device cannot be the root bridge and a secondary root bridge in the same MSTI at the same time.

- There is one and only one root bridge in effect in a spanning tree instance. If two or more devices have been designated to be root bridges of the same spanning tree instance, MSTP will select the device with the lowest MAC address as the root bridge.
- You can specify multiple secondary root bridges for the same instance. Namely, you can specify secondary root bridges for the same instance on two or more than two devices.
- When the root bridge of an instance fails or is shut down, the secondary root bridge (if you have specified one) can take over the role of the primary root bridge. However, if you specify a new primary root bridge for the instance at this time, the secondary root bridge will not become the root bridge. If you have specified multiple secondary root bridges for an instance, when the root bridge fails, MSTP will select the secondary root bridge with the lowest MAC address as the new root bridge.
- Alternatively, you can also specify the current device as the root bridge by setting the priority of the device to 0. For the device priority configuration, refer to Configuring the Priority of the Current Device.

### Configuration example

# Specify the current device as the root bridge of MSTI 1 and a secondary root bridge of MSTI 2.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
[Sysname] stp instance 2 root secondary
```

## Configuring the Work Mode of an MSTP Device

MSTP and RSTP can recognize each other's protocol packets, so they are mutually compatible. However, STP is unable to recognize MSTP packets. For hybrid networking with legacy STP devices and for full interoperability with RSTP-enabled devices, MSTP supports three work modes: STP-compatible mode, RSTP mode, and MSTP mode.

- In STP-compatible mode, all ports of the device send out STP BPDUs,
- In RSTP mode, all ports of the device send out RSTP BPDUs. If the device detects that it is connected with a legacy STP device, the port connecting with the legacy STP device will automatically migrate to STP-compatible mode.
- In MSTP mode, all ports of the device send out MSTP BPDUs. If the device detects that it is connected with a legacy STP device, the port connecting with the legacy STP device will automatically migrate to STP-compatible mode.

### Configuration procedure

Follow these steps to configure the MSTP work mode:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the work mode of MSTP | **stp mode** { **stp** \| **rstp** \| **mstp** } | Optional<br>MSTP mode by default |

### Configuration example

# Configure MSTP to work in STP-compatible mode.

```
<Sysname> system-view
```

```
[Sysname] stp mode stp
```

## Configuring the Priority of the Current Device

The priority of a device determines whether it can be elected as the root bridge of a spanning tree. A lower value indicates a higher priority. By setting the priority of a device to a low value, you can specify the device as the root bridge of the spanning tree. An MSTP-enabled device can have different priorities in different MSTIs.

### Configuration procedure

Follow these steps to configure the priority of the current device in a specified MSTI:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the priority of the current device in a specified MSTI | **stp** [ **instance** *instance-id* ] **priority** *priority* | Optional<br>32768 by default |

**Caution**

- After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.
- During root bridge selection, if all devices in a spanning tree have the same priority, the one with the lowest MAC address will be selected as the root bridge of the spanning tree.

### Configuration example

# Set the device priority in MSTI 1 to 4096.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

## Configuring the Maximum Hops of an MST Region

By setting the maximum hops of an MST region, you can restrict the region size. The maximum hops configured on the regional root bridge will be used as the maximum hops of the MST region.

The regional root bridge always sends a configuration BPDU with a hop count set to the maximum value. When a switch receives this configuration BPDU, it decrements the hop count by 1 and uses the new hop count in the BPDUs it propagates. When the hop count of a BPDU reaches 0, it is discarded by the device that received it. Thus, devices beyond the reach of the maximum hop can no longer take part in spanning tree calculation, and thereby the size of the MST region is confined.

All the devices other than the root bridge in the MST region use the maximum hop value set for the root bridge.

### Configuration procedure

Follow these steps to configure the maximum number of hops of the MST region:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the maximum hops of the MST region | **stp max-hops** *hops* | Optional<br>20 by default |

**Note**

A larger maximum hops setting means a larger size of the MST region. Only the maximum hops configured on the regional root bridge can restrict the size of the MST region.

### Configuration example

# Set the maximum hops of the MST region to 30.

```
<Sysname> system-view
[Sysname] stp max-hops 30
```

## Configuring the Network Diameter of a Switched Network

Any two stations in a switched network are interconnected through a specific path composed of a series of devices. The network diameter is the number of devices on the path composed of the most devices.

### Configuration procedure

Follow these steps to configure the network diameter of the switched network:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the network diameter of the switched network | **stp bridge-diameter** *bridge-number* | Optional<br>7 by default |

**Note**

- The network diameter is a parameter that indicates the network size. A bigger network diameter represents a larger network size.
- Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device.
- The configured network diameter is effective for the CIST only, and not for MSTIs. Each MST region is considered as a device.

### Configuration example

# Set the network diameter of the switched network to 6.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 6
```

## Configuring Timers of MSTP

MSTP involves three timers: forward delay, hello time and max age. You can configure these three parameters for MSTP to calculate spanning trees.

### Configuration procedure

Follow these steps to configure the timers of MSTP:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the forward delay timer | **stp timer forward-delay** *centi-seconds* | Optional<br>1,500 centiseconds (15 seconds) by default |
| Configure the hello timer | **stp timer hello** *centi-seconds* | Optional<br>200 centiseconds (2 seconds) by default |
| Configure the max age timer | **stp timer max-age** *centi-seconds* | Optional<br>2,000 centiseconds (20 seconds) by default |

These three timers set on the root bridge of the CIST apply on all the devices on the entire switched network.

---

**Caution**

- The length of the forward delay time is related to the network diameter of the switched network. Typically, the larger the network diameter is, the longer the forward delay time should be. Note that if the forward delay setting is too small, temporary redundant paths may be introduced; if the forward delay setting is too big, it may take a long time for the network to converge. We recommend that you use the default setting.
- An appropriate hello time setting enables the device to timely detect link failures on the network without using excessive network resources. If the hello time is set too long, the device will take packet loss as a link failure and trigger a new spanning tree calculation process; if the hello time is set too short, the device will send repeated configuration BPDUs frequently, which adds to the device burden and causes waste of network resources. We recommend that you use the default setting.
- If the max age time setting is too small, the network devices will frequently launch spanning tree calculations and may take network congestion as a link failure; if the max age setting is too large, the network may fail to timely detect link failures and fail to timely launch spanning tree calculations, thus reducing the auto-sensing capability of the network. We recommend that you use the default setting.

---

The settings of hello time, forward delay and max age must meet the following formulae; otherwise network instability will frequently occur.

- 2 × (forward delay – 1 second) ⩾ max age
- Max age ⩾ 2 × (hello time + 1 second)

We recommend that you specify the network diameter with the **stp root primary** command and let MSTP automatically calculate optimal settings of these three timers.

### Configuration example

# Set the forward delay to 1,600 centiseconds, hello time to 300 centiseconds, and max age to 2,100 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 1600
[Sysname] stp timer hello 300
[Sysname] stp timer max-age 2100
```

## Configuring the Timeout Factor

After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the downstream devices at the interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.

In a very stable network, this kind of spanning tree calculation may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree calculation by lengthening the timeout time.

### Configuration procedure

Follow these steps to configure the timeout factor:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the timeout factor of the device | **stp timer-factor** *number* | Optional<br>3 by default |

**Note**

- Timeout time = timeout factor × 3 × hello time.
- Typically, we recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

### Configuration example

# Set the timeout factor to 6.

```
<Sysname> system-view
[Sysname] stp timer-factor 6
```

## Configuring the Maximum Port Rate

The maximum rate of a port refers to the maximum number of MSTP packets that the port can send within each hello time. The maximum rate of a port is related to the physical status of the port and the network structure.

### Configuration procedure

Follow these steps to configure the maximum rate of a port or a group of ports:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the maximum rate of the port(s) | | **stp transmit-limit** *packet-number* | Optional<br>10 by default |

**Note**

If the maximum rate setting of a port is too big, the port will send a large number of MSTP packets within each hello time, thus using excessive network resources. We recommend that you use the default setting.

### Configuration example

# Set the maximum transmission rate of port GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

## Configuring Ports as Edge Ports

If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When a network topology change occurs, an edge port will not cause a temporary loop. Because a device does not know whether a port is directly connected to a terminal, you need to manually configure the port to be an edge port. After that, this port can transition rapidly from the blocked state to the forwarding state without delay.

### Configuration procedure

Follow these steps to specify a port or a group of ports as edge port(s):

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the port(s) as edge port(s) | | **stp edged-port enable** | Required<br>All Ethernet ports are non-edge ports by default. |

**Note**

- With BPDU guard disabled, when a port set as an edge port receives a BPDU from another port, it will become a non-edge port again. To restore the edge port, re-enable it.
- If a port directly connects to a user terminal, configure it as an edge port and enable BPDU guard for it. This enables the port to transition to the forwarding state fast while ensuring network security.

### Configuration example

# Configure GigabitEthernet 1/0/1 to be an edge port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port enable
```

## Setting the Link Type of a Port to P2P

A point-to-point link is a link directly connecting two devices. If the two ports across a point-to-point link are root ports or designated ports, the ports can rapidly transition to the forwarding state after a proposal-agreement handshake process.

### Configuration procedure

Follow these steps to set the type of a connected link to P2P:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Set the link type to P2P | | **stp point-to-point** { **auto** \| **force-false** \| **force-true** } | Optional<br>The default setting is **auto**; namely the port automatically detects whether its link is point-to-point. |

**Note**

- A Layer-2 aggregate interface can be configured to connect to a point-to-point link. If a port works in auto-negotiation mode and the negotiation result is full duplex, this port can be configured as connecting to a point-to-point link.
- If a port is configured as connecting to a point-to-point link, the setting takes effect for the port in all MSTIs. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, the configuration may incur a temporary loop.

### Configuration example

# Configure port GigabitEthernet 1/0/1 as connecting to a point-to-point link.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp point-to-point force-true
```

## Configuring the Mode a Port Uses to Recognize/Send MSTP Packets

A port can send/recognize MSTP packets of two formats:

- 802.1s-compliant standard format, and
- Compatible format

By default, the packet format recognition mode of a port is **auto**, namely the port automatically distinguishes the two MSTP packet formats, and determines the format of packets it will send based on the recognized format. You can configure the MSTP packet format to be used by a port. After the configuration, when working in MSTP mode, the port sends and receives only MSTP packets of the format you have configured to communicate with devices that send packets of the same format.

### Configuration procedure

Follow these steps to configure the MSTP packet format to be supported by a port or a group of ports:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the mode the port uses to recognize/send MSTP packets | | **stp compliance** { **auto** \| **dot1s** \| **legacy** } | Optional<br>**auto** by default |

**Note**

- MSTP provides the MSTP packet format incompatibility guard function. In MSTP mode, if a port is configured to recognize/send MSTP packets in a mode other than **auto**, and if it receives a packet in a format different from the specified type, the port will become a designated port and remain in the discarding state to prevent the occurrence of a loop.
- MSTP provides the MSTP packet format frequent change guard function. If a port receives MSTP packets of different formats frequently, this means that the MSTP packet format configuration contains errors. In this case, if the port is working in MSTP mode, it will be disabled for protection. Those ports closed thereby can be restored only by the network administers.

### Configuration example

# Configure GigabitEthernet 1/0/1 to receive and send standard-format MSTP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

## Enabling the Output of Port State Transition Information

In a large-scale, MSTP-enabled network, there are a large number of MSTIs, so ports may frequently transition from one state to another. In this situation, you can enable devices to output the port state transition information of all MSTIs or the specified MSTI so as to monitor the port states in real time.

Follow these steps to enable output of port state transition information:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable output of port state transition information of all MSTIs or a particular MSTI | **stp port-log** { **all \| instance** *instance-id* } | Optional<br>This function is enabled by default. |

## Enabling the MSTP Feature

### Configuration procedure

Follow these steps to enable the MSTP feature:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable the MSTP feature for the device | | **stp enable** | Required<br>By default, MSTP is enabled globally. |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable the MSTP feature for the port(s) | | **stp enable** | Optional<br>By default, MSTP is enabled on all ports. |

**Note**

- MSTP takes effect when it is enabled both globally and on the port.
- You must enable MSTP for the device before any other MSTP-related configuration can take effect.
- To control MSTP flexibly, you can use the **undo stp enable** command to disable the MSTP feature for certain ports so that they will not take part in spanning tree calculation and thus to save the device's CPU resources.

### Configuration example

# Enable MSTP globally and disable MSTP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

# Configuring Leaf Nodes

## Configuring an MST Region

Refer to Configuring an MST Region in the section about root bridge configuration.

## Configuring the Work Mode of MSTP

Refer to Configuring the Work Mode of an MSTP Device in the section about root bridge configuration.

## Configuring the Timeout Factor

Refer to Configuring the Timeout Factor in the section about root bridge configuration.

## Configuring the Maximum Transmission Rate of Ports

Refer to Configuring the Maximum Port Rate in the section about root bridge configuration.

## Configuring Ports as Edge Ports

Refer to Configuring Ports as Edge Ports in the section about root bridge configuration.

## Configuring Path Costs of Ports

Path cost is a parameter related to the rate of a port. On an MSTP-enabled device, a port can have different path costs in different MSTIs. Setting appropriate path costs allows VLAN traffic flows to be forwarded along different physical links, thus to achieve VLAN-based load balancing.

The device can automatically calculate the default path cost; alternatively, you can also configure the path cost for ports.

### Specifying a standard that the device uses when calculating the default path cost

You can specify a standard for the device to use in automatic calculation for the default path cost. The device supports the following standards:

- **dot1d-1998**: The device calculates the default path cost for ports based on IEEE 802.1d-1998.
- **dot1t**: The device calculates the default path cost for ports based on IEEE 802.1t.
- **legacy**: The device calculates the default path cost for ports based on a private standard.

Follow these steps to specify a standard for the device to use when calculating the default path cost:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify a standard for the device to use when calculating the default path costs for ports of the device | **stp pathcost-standard** { **dot1d-1998 \| dot1t** \| **legacy** } | Optional<br>The default standard used by the device is **legacy**. |

**Table 1-7** Link speed vs. path cost

| Link speed | Duplex state | 802.1d-1998 | 802.1t | Private standard |
|---|---|---|---|---|
| 0 | — | 65535 | 200,000,000 | 200,000 |
| 10 Mbps | Single Port | 100 | 2,000,000 | 2,000 |
| | Aggregate Link 2 Ports | 100 | 1,000,000 | 1,800 |
| | Aggregate Link 3 Ports | 100 | 666,666 | 1,600 |
| | Aggregate Link 4 Ports | 100 | 500,000 | 1,400 |
| 100 Mbps | Single Port | 19 | 200,000 | 200 |
| | Aggregate Link 2 Ports | 19 | 100,000 | 180 |
| | Aggregate Link 3 Ports | 19 | 66,666 | 160 |
| | Aggregate Link 4 Ports | 19 | 50,000 | 140 |

| Link speed | Duplex state | 802.1d-1998 | 802.1t | Private standard |
|---|---|---|---|---|
| 1000 Mbps | Single Port | 4 | 20,000 | 20 |
| | Aggregate Link 2 Ports | 4 | 10,000 | 18 |
| | Aggregate Link 3 Ports | 4 | 6,666 | 16 |
| | Aggregate Link 4 Ports | 4 | 5,000 | 14 |
| 10 Gbps | Single Port | 2 | 2,000 | 2 |
| | Aggregate Link 2 Ports | 2 | 1,000 | 1 |
| | Aggregate Link 3 Ports | 2 | 666 | 1 |
| | Aggregate Link 4 Ports | 2 | 500 | 1 |

**Note**

When calculating path cost for an aggregate interface, 802.1d-1998 does not take into account the number of member ports in its aggregation group as 802.1t does. The calculation formula of 802.1t is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregation group.

## Configuring Path Costs of Ports

Follow these steps to configure the path cost of ports:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the path cost of the port(s) | | **stp** [ **instance** *instance-id* ] **cost** *cost* | Required<br>By default, MSTP automatically calculates the path cost of each port. |

**Caution**

- If you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be invalid.
- When the path cost of a port is changed, MSTP will re-calculate the role of the port and initiate a state transition. If you use 0 as *instance-id*, you are setting the path cost of the CIST.

## Configuring Port Priority

The priority of a port is an important factor in determining whether the port can be elected as the root port of a device. If all other conditions are the same, the port with the highest priority will be elected as the root port.

On an MSTP-enabled device, a port can have different priorities in different MSTIs, and the same port can play different roles in different MSTIs, so that data of different VLANs can be propagated along different physical paths, thus implementing per-VLAN load balancing. You can set port priority values based on the actual networking requirements.

### Configuration procedure

Follow these steps to configure the priority of a port or a group of ports:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure a priority for the port(s) | | **stp** [ **instance** *instance-id* ] **port priority** *priority* | Optional<br>128 for all Ethernet ports by default. |

**Note**

- When the priority of a port is changed, MSTP will re-calculate the role of the port and initiate a state transition.
- Generally, a lower configured value indicates a higher priority. If you configure the same priority value for all the ports on a device, the specific priority of a port depends on the index number of the port. Changing the priority of a port triggers a new spanning tree calculation process.

### Configuration example

# Set the priority of port GigabitEthernet 1/0/1 to 16 in MSTI 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 1 port priority 16
```

## Setting the Link Type of a Port to P2P

Refer to Setting the Link Type of a Port to P2P in the section about root bridge configuration.

## Configuring the Mode a Port Uses to Recognize/Send MSTP Packets

Refer to Configuring the Mode a Port Uses to Recognize/Send MSTP Packets in the section about root bridge configuration.

## Enabling Output of Port State Transition Information

Refer to Enabling the Output of Port State Transition Information in the section about root bridge configuration.

## Enabling the MSTP Feature

Refer to Enabling the MSTP Feature in the section about root bridge configuration.

# Performing mCheck

Ports on an MSTP-enabled device have three working modes: STP compatible mode, RSTP mode, and MSTP mode.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, the port on the MSTP (or RSTP) device will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

You can perform mCheck on a port through two approaches, which lead to the same result.

## Configuration Prerequisites

- MSTP has been correctly configured on the device.
- MSTP is configured to operate in MSTP mode or RSTP-compatible mode.

## Configuration Procedure

### Performing mCheck globally

Follow these steps to perform global mCheck:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Perform mCheck | **stp mcheck** | Required |

### Performing mCheck in interface view

Follow these steps to perform mCheck in interface view:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | — |
| Perform mCheck | **stp mcheck** | Required |

## Configuration Example

# Perform mCheck on port GigabitEthernet1/0/1.

1) Method 1: Perform mCheck globally.

```
<Sysname> system-view
[Sysname] stp mcheck
```

2) Method 2: Perform mCheck in interface view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

# Configuring Digest Snooping

As defined in IEEE 802.1s, interconnected devices are in the same region only when the region-related configuration (domain name, revision level, VLAN-to-MSTI mappings) on them is identical. An MSTP enabled device identifies devices in the same MST region via checking the configuration ID in BPDU packets. The configuration ID includes the region name, revision level, configuration digest that is in 16-byte length and is the result calculated via the HMAC-MD5 algorithm based on VLAN-to-MSTI mappings.

Since MSTP implementations differ with vendors, the configuration digests calculated using private keys is different; hence different vendors' devices in the same MST region can not communicate with each other.

Enabling the Digest Snooping feature on the port connecting the local device to another vendor's device in the same MST region can make the two devices communicate with each other.

## Configuration Prerequisites

Associated devices of different vendors are interconnected and run MSTP.

## Configuration Procedure

Follow these steps to configure Digest Snooping:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable digest snooping on the interface or port group | | **stp config-digest-snooping** | Required<br>Not enabled by default |
| Return to system view | | **quit** | — |
| Enable global digest snooping | | **stp config-digest-snooping** | Required<br>Not enabled by default |

**Caution**

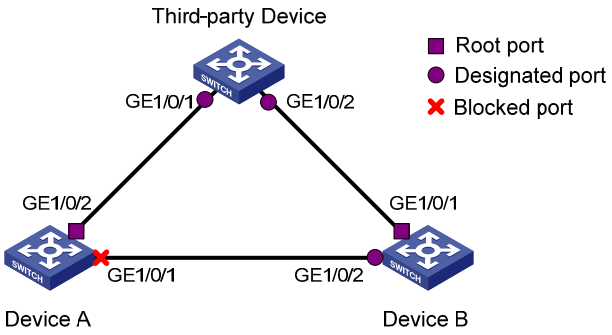
- You can enable Digest Snooping on only a device that is connected to another vendor's device that uses its private key to calculate the configuration digest.
- With the Digest Snooping feature enabled, comparison of configuration digest is not needed for in-the-same-region check, so the VLAN-to-MSTI mappings must be the same on associated ports.
- With global Digest Snooping enabled, modification of VLAN-to-MSTI mappings and removing of the current region configuration using the **undo stp region-configuration** command are not allowed. You can only modify the region name and revision level.
- You need to enable this feature both globally and on associated ports to make it take effect. It is recommended to enable the feature on all associated ports first and then globally, making all configured ports take effect, and disable the feature globally to disable it on all associated ports.
- It is not recommended to enable Digest Snooping on MST region edge ports to avoid loops.
- It is recommended to enable Digest Snooping first and then MSTP. Do not configure Digest Snooping when the network works well to avoid traffic interruption.

## Configuration Example

### Network requirements

- Device A and Device B connect to a third-party's device and all the devices are in the same region.
- Enable Digest Snooping on Device A and Device B so that the three routers can communicate with one another.

**Figure 1-6** Digest Snooping configuration




### Configuration procedure

1) Enable Digest Snooping on Device A.

# Enable Digest Snooping on GigabitEthernet1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
```

# Enable global Digest Snooping.

```
[DeviceA] stp config-digest-snooping
```

2) Enable Digest Snooping on Device B (the same as above, omitted)

## Configuring No Agreement Check

In RSTP and MSTP, two types of messages are used for rapid state transition on designated ports:

- Proposal: sent by designated ports to request rapid transition
- Agreement: used to acknowledge rapid transition requests

Both RSTP and MSTP devices can perform rapid transition on a designated port only when the port receives an agreement packet from the downstream device. The differences between RSTP and MSTP devices are:

- For MSTP, the downstream device's root port sends an agreement packet only after it receives an agreement packet from the upstream device.
- For RSTP, the down stream device sends an agreement packet regardless of whether an agreement packet from the upstream device is received.

Figure 1-7 shows the rapid state transition mechanism on MSTP designated ports.

**Figure 1-7** Rapid state transition of an MSTP designated port

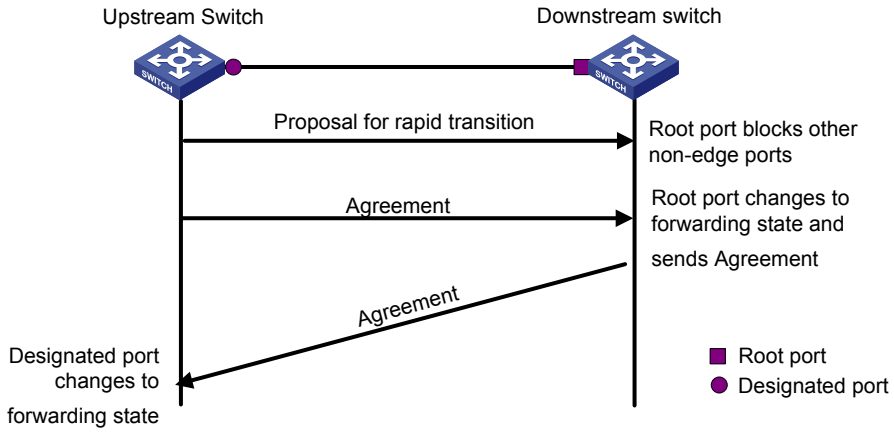
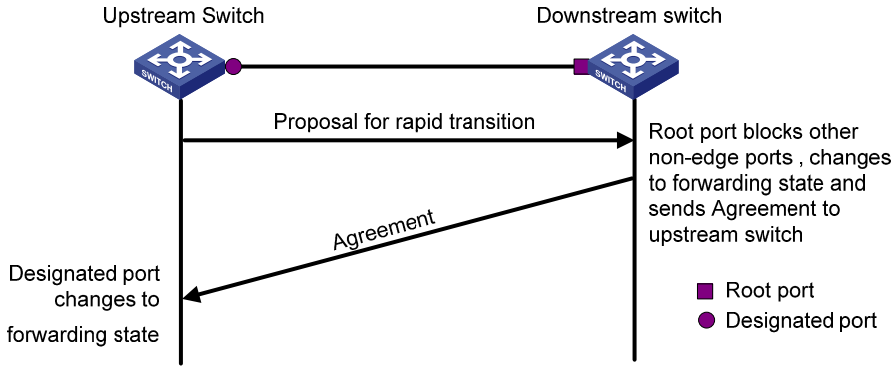



Figure 1-8 shows rapid state transition of an RSTP designated port.

**Figure 1-8** Rapid state transition of an RSTP designated port




If the upstream device comes from another vendor, the rapid state transition implementation may be limited. For example, when the upstream device uses a rapid transition mechanism similar to that of RSTP, and the downstream device adopts MSTP and does not work in RSTP mode, the root port on the downstream device receives no agreement packet from the upstream device and thus sends no agreement packets to the upstream device. As a result, the designated port of the upstream device fails to transit rapidly and can only change to the forwarding state after a period twice the Forward Delay.

In this case, you can enable the No Agreement Check feature on the downstream device's port to enable the designated port of the upstream device to transit its state rapidly.

## Configuration Prerequisites

- A device is connected to an upstream device supporting MSTP via a point-to-point link.
- Configure the same region name, revision level and VLAN-to-MSTI mappings on the two devices, thus assigning them to the same region.

## Configuration Procedure

Follow these steps to configure No Agreement Check:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable No Agreement Check | | **stp no-agreement-check** | Required<br>Not enabled by default |

**Note**

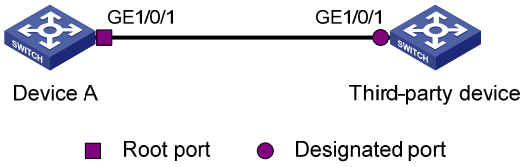
To make the No Agreement Check feature take effect, enable it on the root port.

## Configuration Example

### Network requirements

- Device A connects to a third-party's device that has different MSTP implementation. Both devices are in the same region.
- Another vendor's device is the regional root bridge, and Device A is the downstream device.

**Figure 1-9** No Agreement Check configuration




### Configuration procedure

# Enable No Agreement Check on GigabitEthernet 1/0/1 of Device A.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

# Configuring Protection Functions

An MSTP-enabled device supports the following protection functions:

- BPDU guard
- Root guard

- Loop guard
- TC-BPDU attack guard

---

 **Note**

Among loop guard, root guard and edge port settings, only one function can take effect on the same port at the same time.

---

## Configuration prerequisites

MSTP has been correctly configured on the device.

## Enabling BPDU Guard

---

 **Note**

We recommend that you enable BPDU guard if your device supports this function.

---

For access layer devices, the access ports generally connect directly with user terminals (such as PCs) or file servers. In this case, the access ports are configured as edge ports to allow rapid transition. When these ports receive configuration BPDUs, the system will automatically set these ports as non-edge ports and start a new spanning tree calculation process. This will cause a change of network topology. Under normal conditions, these ports should not receive configuration BPDUs. However, if someone forges configuration BPDUs maliciously to attack the devices, network instability will occur.

MSTP provides the BPDU guard function to protect the system against such attacks. With the BPDU guard function enabled on the devices, when edge ports receive configuration BPDUs, MSTP will close these ports and notify the NMS that these ports have been closed by MSTP. Those ports closed thereby can be restored only by the network administers.

Follow these steps to enable BPDU guard:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the BPDU guard function for the device | **stp bpdu-protection** | Required<br>Disabled by default |

---

 **Note**

BPDU Guard does not take effect on loopback test-enabled ports. For information about loopback test, refer to *Ethernet Interface Configuration* in the *Access Volume*.

---

## Enabling Root Guard

**Note**

We recommend that you enable root guard if your device supports this function.

The root bridge and secondary root bridge of a panning tree should be located in the same MST region. Especially for the CIST, the root bridge and secondary root bridge are generally put in a high-bandwidth core region during network design. However, due to possible configuration errors or malicious attacks in the network, the legal root bridge may receive a configuration BPDU with a higher priority. In this case, the current legal root bridge will be superseded by another device, causing an undesired change of the network topology. As a result, the traffic that should go over high-speed links is switched to low-speed links, resulting in network congestion.

To prevent this situation from happening, MSTP provides the root guard function to protect the root bridge. If the root guard function is enabled on a port of a root bridge, this port will keep playing the role of designated port on all MSTIs. Once this port receives a configuration BPDU with a higher priority from an MSTI, it immediately sets that port to the listening state in the MSTI, without forwarding the packet (this is equivalent to disconnecting the link connected with this port in the MSTI). If the port receives no BPDUs with a higher priority within twice the forwarding delay, the port will revert to its original state.

Follow these steps to enable root guard:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable the root guard function for the port(s) | | **stp root-protection** | Required<br>Disabled by default |

## Enabling Loop Guard

**Note**

We recommend that you enable loop guard if your device supports this function.

By keeping receiving BPDUs from the upstream device, a device can maintain the state of the root port and blocked ports. However, due to link congestion or unidirectional link failures, these ports may fail to receive BPDUs from the upstream devices. In this case, the downstream device will reselect the port roles: those ports in forwarding state that failed to receive upstream BPDUs will become designated ports, and the blocked ports will transition to the forwarding state, resulting in loops in the switched network. The loop guard function can suppress the occurrence of such loops.

If a loop guard–enabled port fails to receive BPDUs from the upstream device, and if the port took part in STP calculation, all the instances on the port, no matter what roles the port plays, will be set to, and stay in, the Discarding state.

Follow these steps to enable loop guard:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>Configurations made in interface view will take effect on the current port only; configurations made in port group view will take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable the loop guard function for the port(s) | | **stp loop-protection** | Required<br>Disabled by default |

## Enabling TC-BPDU Attack Guard

When receiving a TC-BPDU (a BPDU used as notification of a topology change), the device will refresh the forwarding address entries. If someone forges TC-BPDUs to attack the device, the device will receive a larger number of TC-BPDUs within a short time, and frequent refresh operations bring a big burden to the device and hazard network stability.

With the TC-BPDU guard function enabled, the device limits the maximum number of times of immediately refreshing forwarding address entries within 10 seconds after it receives the first TC-BPDUs to the value set with the **stp tc-protection threshold** command (assume the value is X). At the same time, the system monitors whether the number of TC-BPDUs received within that period of time is larger than X. If so, the device will perform another refresh operation after that period of time elapses. This prevents frequent refreshing of forwarding address entries.

Follow these steps to enable TC-BPDU attack guard:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the TC-BPDU attack guard function | **stp tc-protection enable** | Optional<br>Enabled by default |
| Configure the maximum number of times the device refreshes forwarding address entries within a certain period of time immediately after it receives the first TC-BPDU | **stp tc-protection threshold** *number* | Optional<br>6 by default |

**Note**

We recommend that you keep this feature enabled.

## Displaying and Maintaining MSTP

| To do... | Use the command... | Remarks |
|---|---|---|
| View information about abnormally blocked ports | **display stp abnormal-port** | Available in any view |
| View information about ports blocked by STP protection functions | **display stp down-port** | Available in any view |
| View the information of port role calculation history for the specified MSTI or all MSTIs | **display stp** [ **instance** *instance-id* ] **history** | Available in any view |
| View the statistics of TC/TCN BPDUs sent and received by all ports in the specified MSTI or all MSTIs | **display stp** [ **instance** *instance-id* ] **tc** | Available in any view |
| View the status information and statistics information of MSTP | **display stp** [ **instance** *instance-id* ] [ **interface** *interface-list* ] [ **brief** ] | Available in any view |
| View the MST region configuration information that has taken effect | **display stp region-configuration** | Available in any view |
| View the root bridge information of all MSTIs | **display stp root** | Available in any view |
| Clear the statistics information of MSTP | **reset stp** [ **interface** *interface-list* ] | Available in user view |

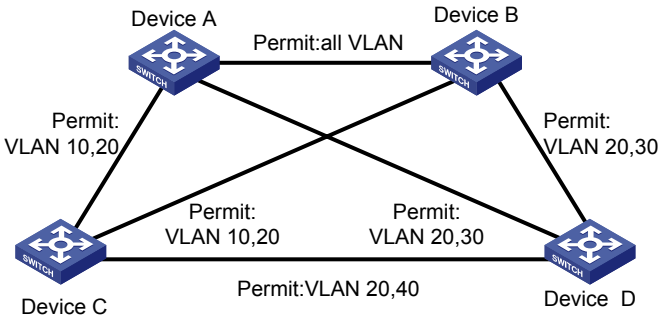
## MSTP Configuration Example

### Network requirements

Configure MSTP so that packets of different VLANs are forwarded along different spanning trees. The specific configuration requirements are as follows:

- All devices on the network are in the same MST region.
- Packets of VLAN 10 are forwarded along MSTI 1, those of VLAN 30 are forwarded along MSTI 3, those of VLAN 40 are forwarded along MSTI 4, and those of VLAN 20 are forwarded along MSTI 0.
- Device A and Device B are distribution layer devices, while Device C and Device D are access layer devices. VLAN 10 and VLAN 30 are terminated on the distribution layer devices, and VLAN 40 is terminated on the access layer devices, so the root bridges of MSTI 1 and MSTI 3 are Device A and Device B respectively, while the root bridge of MSTI 4 is Device C.

**Figure 1-10** Network diagram for MSTP configuration




---

**Note**

"Permit:" beside each link in the figure is followed by the VLANs the packets of which are permitted to pass this link.

---

## Configuration procedure

1) Configuration on Device A

# Enter MST region view.

```
<DeviceA> system-view
[DeviceA] stp region-configuration
```

# Configure the region name, VLAN-to-MSTI mappings and revision level of the MST region.

```
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
[DeviceA-mst-region] revision-level 0
```

# Activate MST region configuration manually.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Define Device A as the root bridge of MSTI 1.

```
[DeviceA] stp instance 1 root primary
```

# Enable MSTP globally.

```
[DeviceA] stp enable
```

# View the MST region configuration information that has taken effect.

```
[DeviceA] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :example
   Revision level     :0

   Instance   Vlans Mapped
```

```
      0       1 to 9, 11 to 29, 31 to 39, 41 to 4094
      1       10
      3       30
      4       40
```

2) Configuration on Device B

# Enter MST region view.

```
<DeviceB> system-view
[DeviceB] stp region-configuration
```

# Configure the region name, VLAN-to-MSTI mappings and revision level of the MST region.

```
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
[DeviceB-mst-region] revision-level 0
```

# Activate MST region configuration manually.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Define Device B as the root bridge of MSTI 3.

```
[DeviceB] stp instance 3 root primary
```

# Enable MSTP globally.

```
[DeviceB] stp enable
```

# View the MST region configuration information that has taken effect.

```
[DeviceB] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :example
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 29, 31 to 39, 41 to 4094
      1       10
      3       30
      4       40
```

3) Configuration on Device C.

# Enter MST region view.

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

# Configure the region name, VLAN-to-MSTI mappings and revision level of the MST region.

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
[DeviceC-mst-region] revision-level 0
```

# Activate MST region configuration manually.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Define Device C as the root bridge of MSTI 4.

```
[DeviceC] stp instance 4 root primary
```

# Enable MSTP globally.

```
[DeviceC] stp enable
```

# View the MST region configuration information that has taken effect.

```
[DeviceC] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :example
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 29, 31 to 39, 41 to 4094
      1       10
      3       30
      4       40
```

4) Configuration on Device D.

# Enter MST region view.

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
```

# Configure the region name, VLAN-to-MSTI mappings and revision level of the MST region.

```
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
[DeviceD-mst-region] revision-level 0
```

# Activate MST region configuration manually.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Enable MSTP globally.

```
[DeviceD] stp enable
```

# View the MST region configuration information that has taken effect.

```
[DeviceD] display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :example
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 29, 31 to 39, 41 to 4094
      1       10
      3       30
```

```
4       40
```

# Table of Contents

# 1 Smart Link Configuration

When configuring Smart Link, go to these sections for information that you are interested in:



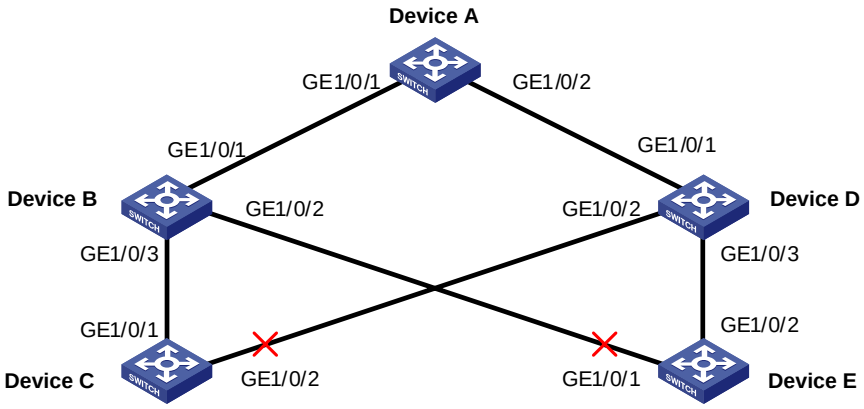
## Smart Link Overview

Smart Link is a feature developed to address the slow convergence issue with the Spanning Tree Protocol (STP). (For information about STP, refer to *MSTP Configuration* in the *Access Volume*.)

Smart Link is dedicated to dual-uplink networks as shown in Figure 1-1 to provide link redundancy with subsecond convergence. It allows the backup link to take over quickly when the primary link fails. In addition to fast convergence, Smart Link is easy to configure.

### Terminology

**Figure 1-1** Smart Link application scenario




#### Smart link group

A smart link group consists of only two member ports: the master and the slave. At a time, only one port is active for forwarding, and the other port is blocked, that is, in the standby state. When link failure occurs on the active port due to port shutdown or presence of unidirectional link for example, the standby port becomes active to take over while the original active port transits to the blocked state.

As shown in Figure 1-1, GE1/0/1 and GE1/0/2 of Device C form a smart link group, with GE1/0/1 being active and GE1/0/2 being standby. GE1/0/1 and GE1/0/2 of Device E form another smart link group, with GE1/0/2 being active and GE1/0/1 being standby.

### Master port

Master port is a port role in a smart link group. When both ports in a smart link group are up, the master port preferentially transits to the forwarding state. Once the master port fails, the slave port takes over to forward traffic. During this period, if the smart link group is not configured with role preemption, the master port stays in standby state until the next link switchover even if it has recovered.

As shown in Figure 1-1, you can configure GE1/0/1 of Device C and GE1/0/2 of Device E as master ports.

### Slave port

Slave port is a port role in a smart link group. When both ports in a smart link group are up, the slave port is placed in the standby state. When the master port fails, the slave port takes over to forward traffic.

As shown in Figure 1-1, you can configure GE1/0/2 of Device C and GE1/0/1 of Device E as slave ports.

### Flush message

Flush messages are used by a smart link group to notify other devices to refresh their MAC address forwarding entries and ARP/ND entries when link switchover occurs in the smart link group. Flush messages are common multicast data packets, and will be dropped by a blocked receiving port.

### Transmit control VLAN

The transmit control VLAN is used for transmitting flush messages. When link switchover occurs, the devices (such as Device C and E in Figure 1-1) broadcast flush messages within the transmit control VLAN.

### Receive control VLAN

The receive control VLAN is used for receiving and processing flush messages. When link switchover occurs, the devices (such as Device A, B, and D in Figure 1-1) receive and process flush messages in the receive control VLAN and refresh their MAC address forwarding entries and ARP/ND entries.

### Protected VLAN

A smart link group controls the forwarding state of some data VLANs, which are referred to as protected VLANs. Different smart link groups on a port control different protected VLANs. The state of the port in a protected VLAN is determined by the state of the port in the smart link group.

## Operating Mechanism of Smart Link

### Link backup mechanism

As shown in Figure 1-1, the link on GE1/0/1 of Device C is the active link, and the link on GE1/0/2 of Device C is the standby link. Normally, GE1/0/1 is in the forwarding state, while GE1/0/2 is in the standby state. When the link on GE1/0/1 fails, GE1/0/2 takes over to forward traffic while GE1/0/1 is blocked and placed in the standby state.

When a port switches to the forwarding state, the system outputs log information to notify the user of the port state change.

As link switchover can outdate the MAC address forwarding entries and ARP/ND entries on all devices, you need a forwarding entry update mechanism to ensure proper transmission. By far, the following two update mechanisms are provided:

- Uplink traffic-triggered MAC address learning, where update is triggered by uplink traffic. This mechanism is applicable to environments with devices not supporting smart link, including devices of other vendors'.
- Flush update where a Smart Link-enabled device updates its information by transmitting flush messages over the backup link to its upstream devices. This mechanism requires the upstream devices to be capable of recognizing smart link flush messages to update its MAC address forwarding entries and ARP/ND entries.

To keep traffic forwarding stable, the master port that has been blocked due to link failure does not take over immediately upon its recovery. Instead, link switchover will occur at next link switchover.

### Role preemption mechanism

As shown in Figure 1-1, the link on GE1/0/1 of Device C is the active link, and the link on GE1/0/2 of Device C is the standby link. Once GE1/0/1 fails, GE1/0/2 takes over to forward traffic. During this period, if the smart link group is configured with role preemption, GE1/0/1 takes over to forward traffic as soon as it recovers.

### Load sharing mechanism

A ring network may carry traffic of multiple VLANs. Smart link can forward traffic of different VLANs in different smart link groups, thus implementing load sharing.

To implement load sharing, you can assign a port to multiple smart link groups (each configured with different protected VLANs), making sure that the state of the port is different in these smart link groups. In this way, traffic of different VLANs can be forwarded along different paths.

You can configure protected VLANs for a smart link group by referencing MSTIs.

# Configuring a Smart Link Device

To use Smart Link on a device, you must configure the device with a smart link group and transmit control VLAN for flush message transmission. Device C and Device E in Figure 1-1 are two examples of Smart Link devices.

## Configuration Prerequisites

- Before configuring a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable STP and RRPP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group.

## Configuring a Smart Link Device

Follow these steps to configure a smart link device:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a smart link group and enter smart link group view | **smart-link group** *group-id* | Required |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure protected VLANs for the smart link group | | **protected-vlan reference-instance** *instance-id-list* | Required<br>By default, no protected VLAN is configured for a smart link group. |
| Specify the master port for the smart link group | In smart link group view | **port** *interface-type interface-number* **master** | Required<br>Use either approach. |
| | In Ethernet interface view or Layer-2 aggregate interface view | **port smart-link group** *group-id* **master** | |
| Specify the slave port for the smart link group | In smart link group view | **port** *interface-type interface-number* **slave** | Required<br>Use either approach. |
| | In Ethernet interface view or Layer-2 aggregate interface view | **port smart-link group** *group-id* **slave** | |
| Enable role preemption | | **preemption mode role** | Optional<br>Disabled by default. |
| Configure the preemption delay | | **preemption delay** *delay-time* | Optional<br>1 second by default. |
| Enable flush update in the specified control VLAN | | **flush enable** [ **control-vlan** *vlan-id* ] | Optional<br>By default, VLAN 1 is used for flush update. |

**Caution**

- The **protected-vlan** command configures protected VLANs for a smart link group by referencing MSTIs. To view VLAN-to-MSTI mappings, use the **display stp region-configuration** command. For VLAN-to-MSTI mapping configuration, refer to *MSTP Configuration* in the *Access Volume*.
- The preemption delay configuration takes effect only after preemption mode is enabled.
- The protected VLANs configured for a smart link group must be different from those configured for any other smart link group.
- Make sure that the configured control VLANs are existing VLANs, and you must assign the smart link group member ports to the control VLANs.
- Do not remove the control VLANs. Otherwise, flush messages cannot be sent properly.

## Smart Link Device Configuration Example

### Network requirements

- Create smart link group 1.
- The protected VLANs of smart link group 1 are mapped to MSTI 0 through 8.
- Configure GigabitEthernet 1/0/1 as the master port of the smart link group, and GigabitEthernet 1/0/2 as the slave port.

- Configure VLAN 20 for flush update.

### Configuration procedure

```
<Sysname> system-view
[Sysname] vlan 20
[Sysname-vlan20] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 20
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] undo stp enable
[Sysname-GigabitEthernet1/0/2] port link-type trunk
[Sysname-GigabitEthernet1/0/2] port trunk permit vlan 20
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0 to 8
[Sysname-smlk-group1] port gigabitethernet1/0/1 master
[Sysname-smlk-group1] port gigabitethernet1/0/2 slave
[Sysname-smlk-group1] flush enable control-vlan 20
```

# Configuring an Associated Device

The active and standby links in a smart link group may traverse multiple devices between the Smart Link device and the destination device. For Smart Link to work, you need to enable all the ports on the way to the destination to process the flush messages sent from the smart link device.

For example, as all the numbered ports on Device A, B, and D in Figure 1-1 are on the way of the active and standby links from Device C and E to Device A, you need to enable the ports to process flush messages received from the control VLAN configured on Device C and E.

## Configuring an Associated Device

Follow these steps to configure an associated device:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | — |
| Configure the control VLAN for receiving flush messages | **smart-link flush enable** [ **control-vlan** *vlan-id-list* ] | Required<br>No control VLAN exists for receiving flush messages of Smart Link by default. |

**Caution**

- Configure all the control VLANs to receive flush messages.
- If no control VLAN is specified for processing flush messages, the device forwards the received flush messages directly without processing them.
- Make sure that the receive control VLAN is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages directly without any processing.
- Do not remove the control VLANs. Otherwise, flush messages cannot be sent properly.
- Make sure that the control VLANs are existing VLANs, and you must assign the port capable of receiving flush messages to the control VLANs.

### Associated Device Configuration Example

#### Network requirements

Configure GigabitEthernet 1/0/1 to receive and process flush messages in VLAN 20.

#### Configuration procedure

```
<Sysname> system-view
[Sysname] vlan 20
[Sysname-vlan20] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 20
[Sysname-GigabitEthernet1/0/1] smart-link flush enable control-vlan 20
```

## Displaying and Maintaining Smart Link

| To do... | Use the command… | Remarks |
|---|---|---|
| Display smart link group information | **display smart-link group** { *group-id* \| **all** } | Available in any view |
| Display information about the received flush messages | **display smart-link flush** | Available in any view |
| Clear the statistics about flush messages | **reset smart-link statistics** | Available in user view |

## Smart Link Configuration Examples

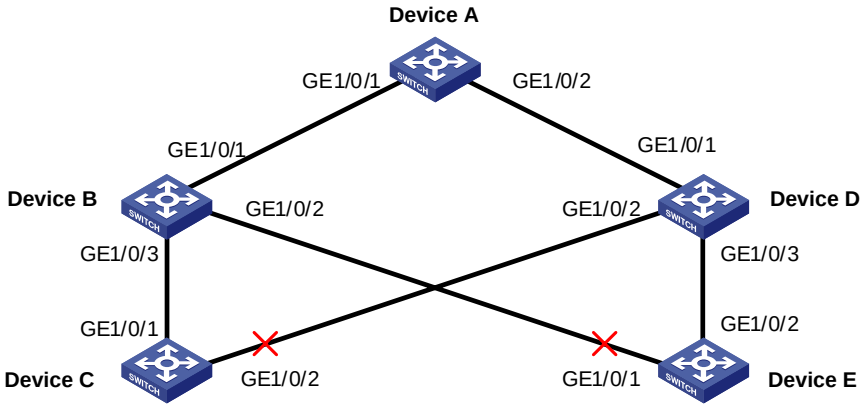
### Single Smart Link Group Configuration Example

#### Network requirements

As shown in Figure 1-2, both Device C and Device E are dually uplinked to Device A.

Configure Smart Link on the devices for uplink backup, adopting VLAN 1 (the default) for flush update.

**Figure 1-2** Network diagram for single smart link group configuration




## Configuration procedure

1) Configuration on Device C

# Create smart link group 1.

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] smart-link group 1
```

# Configure all VLANs mapped to MSTIs 0 through 16 as the protected VLANs.

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0 to 16
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port.

```
[DeviceC-smlk-group1] port gigabitethernet1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet1/0/2 slave
```

# Configure VLAN 1 as the transmit control VLAN.

```
[DeviceC-smlk-group1] flush enable
```

2) Configuration on Device E

# Create smart link group 1.

```
<DeviceE> system-view
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] quit
[DeviceE] smart-link group 1
```

# Configure all VLANs mapped to MSTIs 0 through 16 as the protected VLANs.

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0 to 16
```

# Configure GigabitEthernet 1/0/2 as the master port and GigabitEthernet 1/0/1 as the slave port.

```
[DeviceE-smlk-group1] port gigabitethernet1/0/2 master
[DeviceE-smlk-group1] port gigabitethernet1/0/1 slave
```

# Configure VLAN 1 as the transmit control VLAN.

```
[DeviceE-smlk-group1] flush enable
```

3) Configuration on Device B

# Configure VLAN 1 as the receive control VLAN for GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable
```

4) Configuration on Device D

# Configure VLAN 1 as the receive control VLAN for GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
<DeviceD> system-view
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] smart-link flush enable
```

5) Configuration on Device A

# Configure VLAN 1 as the receive control VLAN for GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
```

After completing the configuration, you can use the **display** command to verify the smart link configuration and view flush message statistics.

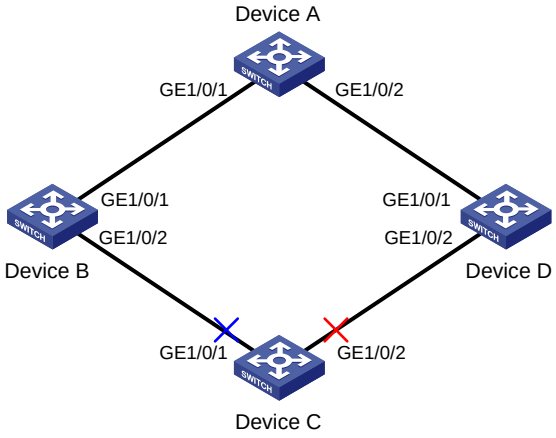
## Multiple Smart Link Groups Load Sharing Configuration Example

### Network requirements

As shown in Figure 1-3:

- The traffic of VLAN 1 through VLAN 200 on Device C are dually uplinked to Device A by Device B and Device D. Implement load sharing to uplink the traffic of VLAN 1 through VLAN 100 and the traffic of VLAN 101 through VLAN 200 over different links to Device A.
- Implement dual link backup on Device C: the traffic of VLANs 1 through 100 (mapped to MSTI 0) is uplinked to Device A by Device B; the traffic of VLANs 101 through 200 (mapped to MSTI 2) is uplinked to Device A by Device D. Smart link group 1 references MSTI 0, and smart link group 2 references MSTI 2.
- The control VLAN of smart link group 1 is VLAN 10 and that of smart link group 2 is VLAN 101.

**Figure 1-3** Network diagram for multiple smart link groups load sharing configuration




## Configuration procedure

1) Configuration on Device C

# Create VLANs and configure VLAN-to-MSTI mappings.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 0 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Disable STP on the ports, configure the ports as trunk ports, and configure the ports to allow packets from VLAN 1 through 200 to pass through.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1.

```
[DeviceC] smart-link group 1
```

# Configure protected VLANs for smart link group 1.

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port.

```
[DeviceC-smlk-group1] port gigabitethernet1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet1/0/2 slave
```

# Enable role preemption.

```
[DeviceC-smlk-group1] preemption mode role
```

# Configure VLAN 10 as the transmit control VLAN of smart link group 1.

```
[DeviceC-smlk-group-1] flush enable control-vlan 10
[DeviceC-smlk-group-1] quit
```

# Create smart link group 2.

```
[DeviceC] smart-link group 2
```

# Configure protected VLANs for smart link group 2.

```
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

# Configure GigabitEthernet 1/0/1 as the slave port and GigabitEthernet 1/0/2 as the master port.

```
[DeviceC-smlk-group2] port gigabitethernet1/0/1 slave
[DeviceC-smlk-group2] port gigabitethernet1/0/2 master
```

# Enable role preemption.

```
[DeviceC-smlk-group2] preemption mode role
```

# Configure VLAN 101 as the transmit control VLAN of smart link group 2.

```
[DeviceC-smlk-group2] flush enable control-vlan 101
```

2) Configuration on Device B

# Configure VLAN 10 and VLAN 101 as the receive control VLANs of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
```

3) Configuration on Device D

# Configure VLAN 10 and VLAN 101 as the receive control VLANs of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
```

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
```

4) Configuration on Device A

# Configure VLAN 10 and VLAN 101 as the receive control VLANs of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
```

After completing the configuration, you can use the **display** command to verify the smart link configuration and view flush message statistics.

# Table of Contents

# 1 Monitor Link Configuration

When configuring monitor link, go to these sections for information you are interested in:



## Overview

Monitor link is a port collaboration function used to enable a device to be aware of the up/down state change of the ports on an indirectly connected link. Monitor link is usually used in conjunction with Layer-2 topology protocols. The idea is to adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switchover on the downlink device in time.

### Terminology

#### Monitor link group

A monitor link group is a set of uplink ports and downlink ports. For the purpose of monitor link, uplink ports refer to the monitored ports while downlink ports refer to the ports adapted to the up/down state of the monitored ports. A port can be assigned to only one monitor link group. Both Layer-2 Ethernet ports and Layer-2 aggregate interfaces can be assigned to a monitor link group.

#### Uplink

The uplink is the link monitored by the monitor link group. The monitor link group is down when the group has no uplink ports or all uplink ports are down. The monitor link group is up when any uplink port is up.

#### Downlink

The downlink is the state-adaptive link in the monitor link group. The state of the downlink ports is always consistent with the up/down state of the monitor link group.

### How Monitor Link Works

A monitor link group works independently of other monitor link groups. When a monitor link group contains no uplink ports or all its uplink ports go down, the monitor link group goes down and forces all downlink ports down at the same time. When any uplink port goes up, the monitor link group goes up and brings up all the downlink ports.

**Caution**

Do not manually shut down or bring up the downlink ports in a monitor link group.

# Configuring Monitor Link

## Configuration Prerequisites

Before assigning a port to a monitor link group, make sure the port is not the member port of any aggregation group.

## Configuration Procedure

Follow these steps to configure monitor link:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a monitor link group and enter monitor link group view | | **monitor-link group** *group-id* | Required |
| Configure the uplink for the monitor link group | In monitor link group view | **port** *interface-type interface-number* **uplink** | Use either approach<br>Repeat this step to add more uplink ports |
| | In Ethernet port view or Layer-2 aggregate interface view | **port monitor-link group** *group-id* **uplink** | |
| Configure the downlink for the monitor link group | In monitor link group view | **port** *interface-type interface-number* **downlink** | Use either approach<br>Repeat this step to add more downlink ports |
| | In Ethernet port view or Layer-2 aggregate interface view | **port monitor-link group** *group-id* **downlink** | |

**Caution**

- A port can be assigned to only one monitor link group.
- You are recommended to configure uplink ports prior to downlink ports, thus avoiding undesired down/up state changes on the downlink ports.

## Monitor Link Configuration Example

### Network requirements

GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of a device are up. Configure GigabitEthernet 1/0/2 to change its up/down state as GigabitEthernet 1/0/1.

### Configuration procedure

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

## Displaying and Maintaining Monitor Link

| To do… | Use the command… | Remarks |
|---|---|---|
| Display monitor link group information | **display monitor-link group** { *group-id* **\| all** } | Available in any view |

## Monitor Link Configuration Example

### Network requirements

As shown in Figure 1-1:

- Device C is dually uplinked to Device A through a smart link group.
- It is required that when GigabitEthernet 1/0/1 or GigabitEthernet 1/0/2 of Device A fails, Device C can sense the link failure and perform link switchover in the smart link group.

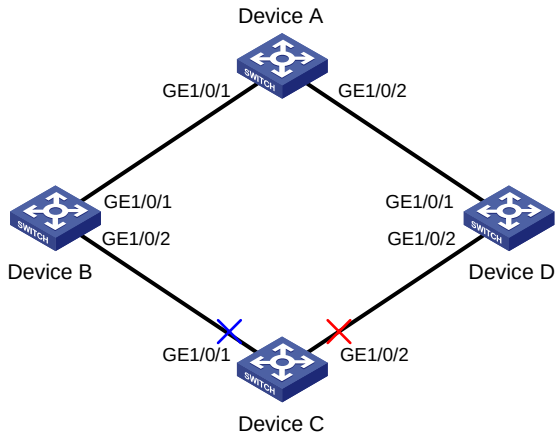
---

**Note**

For detailed information about smart link, refer to *Smart Link Configuration* in the *Access Volume*.

---

**Figure 1-1** Network diagram for smart link in combination with monitor link configuration




### Configuration procedure

1) Configuration on Device C

# Create smart link group 1.

```
<DeviceC> system-view
```

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] smart-link group 1
```

# Configure the smart link group to protect all the VLANs mapped to MSTIs 0 through 16.

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0 to 16
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port.

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

# Enable the smart link group to transmit flush messages in VLAN 1.

```
[DeviceC-smlk-group1] flush enable
```

2) Configuration on Device A

# Configure VLAN 1 as the control VLAN for receiving flush messages on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
```

3) Configuration on Device B

# Create monitor link group 1.

```
<DeviceB> system-view
[DeviceB] monitor-link group 1
```

# Configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port.

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

# Configure VLAN 1 as the control VLAN for receiving flush messages on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceB-mtlk-group-1] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
```

4) Configuration on Device D

# Create monitor link group 1.

```
<DeviceD> system-view
[DeviceD] monitor-link group 1
```

# Configure GigabitEthernet 1/0/1 as the uplink port and GigabitEthernet 1/0/2 as the downlink port.

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

# Configure VLAN 1 as the control VLAN for receiving flush messages on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceD-mtlk-group1] quit
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
```

# Table of Contents

# 1 VLAN Configuration

When configuring VLAN, go to these sections for information you are interested in:



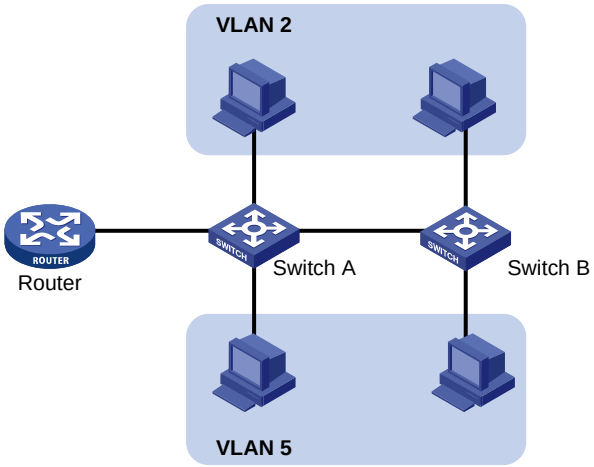
## Introduction to VLAN

### VLAN Overview

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared, collisions and excessive broadcasts cannot be avoided on an Ethernet. To address the issue, virtual LAN (VLAN) was introduced.

The idea is to break a LAN down into separate VLANs, that is, Layer 2 broadcast domains whereby frames are switched between ports assigned to the same VLAN. VLANs are isolated from each other at Layer 2. A VLAN is a bridging domain, and all broadcast traffic is contained within it, as shown in Figure 1-1.

**Figure 1-1** A VLAN diagram




A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same LAN, regardless of their physical locations.

VLAN technology delivers the following benefits:

1) Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
2) Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
3) Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

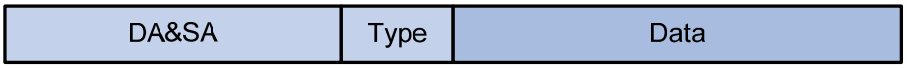
## VLAN Fundamentals

To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

The format of VLAN-tagged frames is defined in IEEE 802.1Q issued by IEEE in 1999.

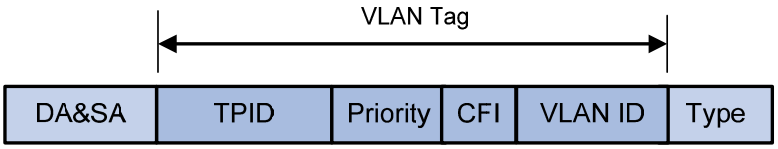
In the header of a traditional Ethernet data frame, the field after the destination MAC address and the source MAC address is the Type field indicating the upper layer protocol type, as shown in Figure 1-2.

**Figure 1-2** The format of a traditional Ethernet frame




IEEE 802.1Q inserts a four-byte VLAN tag after the DA&SA field, as shown in Figure 1-3.

**Figure 1-3** The position and format of VLAN tag




A VLAN tag comprises four fields: tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN-tagged.
- The 3-bit priority field indicates the 802.1p priority of the frame. For information about frame priority, refer to *QoS Configuration* in the *QoS Volume*.
- The 1-bit CFI field specifies whether the MAC addresses are encapsulated in the standard format when packets are transmitted across different media. Value 0 indicates that MAC addresses are encapsulated in the standard format; value 1 indicates that MAC addresses are encapsulated in a non-standard format. The filed is 0 by default.
- The 12-bit VLAN ID field identifies the VLAN the frame belongs to. The VLAN ID range is 0 to 4095. As 0 and 4095 are reserved by the protocol, a VLAN ID actually ranges from 1 to 4094.

When receiving a frame, a network device handles the frame depending on whether the frame is VLAN tagged and the value of the VLAN tag, if any. For more information, refer to section Introduction to Port-Based VLAN.

**Note**

- The Ethernet II encapsulation format is used here. Besides the Ethernet II encapsulation format, other encapsulation formats, including 802.2 LLC, 802.2 SNAP, and 802.3 raw, are also supported by Ethernet. The VLAN tag fields are also added to frames encapsulated in these formats for VLAN identification.
- For a frame with multiple VLAN tags, the device handles it according to its outer VLAN tag, while transmits its inner VLAN tags as payload.

### Types of VLAN

You can implement VLAN based on:

- Port
- MAC address
- Protocol
- IP subnet
- Policy
- Other criteria

This chapter covers port-based VLAN, MAC-based VLAN, protocol-based VLAN, and IP-based VLAN. You can configure the four types of VLANs on a port at the same time. When determining to which VLAN a packet passing through the port should be assigned, the device looks up the VLANs in the default order of MAC-based VLANs, IP-based VLANs, protocol-based VLANs, and port-based VLANs.

## Configuring Basic VLAN Settings

Follow these steps to configure basic VLAN settings:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create VLANs | **vlan** { *vlan-id1* [ **to** *vlan-id2* ] \| **all** } | Optional<br>Using this command can create multiple VLANs in bulk. |
| Enter VLAN view | **vlan** *vlan-id* | Required<br>If the specified VLAN does not exist, this command creates the VLAN first.<br>By default, only the default VLAN (that is, VLAN 1) exists in the system. |
| Configure a name for the current VLAN | **name** *text* | Optional<br>By default, the name of a VLAN is its VLAN ID, **VLAN 0001** for example. |
| Configure the description of the current VLAN | **description** *text* | Optional<br>VLAN ID is used by default, for example, **VLAN 0001**. |

**Note**

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot manually create or remove VLANs reserved for special purposes.
- Dynamic VLANs cannot be removed with the **undo vlan** command.
- A VLAN with a QoS policy applied cannot be removed.
- For isolate-user-VLANs or secondary VLANs, if you have used the **isolate-user-vlan** command to create mappings between them, you cannot remove them until you remove the mappings between them first.
- A VLAN operating as a probe VLAN for remote port mirroring cannot be removed with the undo vlan command. To do that, remove the remote mirroring VLAN configuration from it first.

## Configuring Basic Settings of a VLAN Interface

For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, VLAN interfaces are used.

VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface. You can assign the VLAN interface an IP address and specify it as the gateway of the VLAN to forward traffic destined for an IP network segment different from that of the VLAN.

Follow these steps to configure basic settings of a VLAN interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a VLAN interface and enter VLAN interface view | **interface vlan-interface** *vlan-interface-id* | Required<br>If the VLAN interface already exists, you enter its view directly. |
| Assign an IP address to the VLAN interface | **ip address** *ip-address* { *mask* \| *mask-length* } [ **sub** ] | Optional<br>No IP address is assigned to any VLAN interface by default. |
| Configure the description of the VLAN interface | **description** *text* | Optional<br>VLAN interface name is used by default, for example, **Vlan-interface1 Interface.** |
| Bring up the VLAN interface | **undo shutdown** | Optional<br>By default, a VLAN interface is in the up state. In this case, the VLAN interface is up so long as one port in the VLAN is up and goes down if all ports in the VLAN go down.<br>An administratively shut down VLAN interface however will be in the down state until you bring it up, regardless of how the state of the ports in the VLAN changes. |

**Note**

Before creating a VLAN interface for a VLAN, create the VLAN first.

# Port-Based VLAN Configuration

## Introduction to Port-Based VLAN

Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

### Port link type

You can configure the link type of a port as access, trunk, or hybrid. The three link types use different VLAN tag handling methods. When configuring the link type of a port, note that:

- An access port can belong to only one VLAN. Usually, ports directly connected to PCs are configured as access ports.
- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic of the default VLAN, traffic passes through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports to allow members of the same VLAN to communicate with each other across multiple network devices.
- Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through VLAN untagged. You can configure a port connected to a network device or user terminal as a hybrid port for access link connectivity or trunk connectivity.

### Default VLAN

By default, VLAN 1 is the default VLAN for all ports. You can configure the default VLAN for a port as required.

Use the following guidelines when configuring the default VLAN on a port:

- Because an access port can join only one VLAN, its default VLAN is the VLAN to which it belongs and cannot be configured.
- Because a trunk or hybrid port can join multiple VLANs, you can configure a default VLAN for the port.
- You can use a nonexistent VLAN as the default VLAN for a hybrid or trunk port but not for an access port. Therefore, after you remove the VLAN that an access port resides in with the **undo vlan** command, the default VLAN of the port changes to VLAN 1. The removal of the VLAN specified as the default VLAN of a trunk or hybrid port, however, does not affect the default VLAN setting on the port.

**Note**

- Do not set the voice VLAN as the default VLAN of a port in automatic voice VLAN assignment mode. Otherwise, the system prompts error information. For information about voice VLAN, refer to Voice VLAN Configuration.
- The local and remote ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

A port configured with the default VLAN handles a frame as follows:

| Port type | Actions (in the inbound direction) | | Actions (in the outbound direction) |
|---|---|---|---|
| | Untagged frame | Tagged frame | |
| Access | Tag the frame with the default VLAN tag. | • Receive the frame if its VLAN ID is the same as the default VLAN ID.<br>• Drop the frame if its VLAN ID is different from the default VLAN ID. | Remove the default VLAN tag and send the frame. |
| Trunk | Check whether the default VLAN is permitted on the port:<br>• If yes, tag the frame with the default VLAN tag.<br>• If not, drop the frame. | • Receive the frame if its VLAN is carried on the port.<br>• Drop the frame if its VLAN is not carried on the port. | • Remove the tag and send the frame if the frame carries the default VLAN tag.<br>• Send the frame without removing the tag if its VLAN is carried on the port but is different from the default one. |
| Hybrid | | | Send the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration with the **port hybrid vlan** command. This is true of the default VLAN. |

## Assigning an Access Port to a VLAN

You can assign an access port to a VLAN in VLAN view, interface view, or port group view.

1) In VLAN view

Follow these steps to assign one or multiple access ports to a VLAN in VLAN view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | Required<br>If the specified VLAN does not exist, this command creates the VLAN first. |
| Assign one or a group of access ports to the current VLAN | **port** *interface-list* | Required<br>By default, all ports belong to VLAN 1. |

2) In interface or port group view

Follow these steps to assign an access port (in interface view) or multiple access ports (in port group view) to a VLAN:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In port group view, the subsequent configurations apply to all ports in the port group.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the link type of the port or ports as access | | **port link-type access** | Optional<br>The link type of a port is access by default. |
| Assign the current access port(s) to a VLAN | | **port access vlan** *vlan-id* | Optional<br>By default, all access ports belong to VLAN 1. |

**Note**

- Before assigning an access port to a VLAN, create the VLAN first.
- After you configure a command on a Layer-2 aggregate interface, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port.

## Assigning a Trunk Port to a VLAN

A trunk port can carry multiple VLANs. You can assign it to a VLAN in interface view or port group view.

Follow these steps to assign a trunk port to one or multiple VLANs:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In port group view, the subsequent configurations apply to all ports in the port group.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the link type of the port or ports as trunk | | **port link-type trunk** | Required |
| Assign the trunk port(s) to the specified VLAN(s) | | **port trunk permit vlan** { *vlan-id-list* \| **all** } | Required<br>By default, a trunk port carries only VLAN 1. |
| Configure the default VLAN of the trunk port(s) | | **port trunk pvid vlan** *vlan-id* | Optional<br>VLAN 1 is the default VLAN by default. |

**Note**

- To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.
- The local and remote hybrid ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a trunk port, you must use the **port trunk permit vlan** command to configure the trunk port to allow packets from the default VLAN to pass through, so that the egress port can forward packets from the default VLAN.
- After you configure a command on a Layer-2 aggregate interface, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port.

## Assigning a Hybrid Port to a VLAN

A hybrid port can carry multiple VLANs. You can assign it to a VLAN in interface view or port group view.

Follow these steps to assign a hybrid port to one or multiple VLANs:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In port group view, the subsequent configurations apply to all ports in the port group.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the link type of the port(s) as hybrid | | **port link-type hybrid** | Required |
| Assign the hybrid port(s) to the specified VLAN(s) | | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required<br>By default, a hybrid port allows only packets of VLAN 1 to pass through untagged. |
| Configure the default VLAN of the hybrid port | | **port hybrid pvid vlan** *vlan-id* | Optional<br>VLAN 1 is the default by default. |

**Note**

- To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.
- Before assigning a hybrid port to a VLAN, create the VLAN first.
- The local and remote hybrid ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a hybrid port, you must use the **port hybrid vlan** command to configure the hybrid port to allow packets from the default VLAN to pass through, so that the egress port can forward packets from the default VLAN.
- After you configure a command on a Layer-2 aggregate interface, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port.

# MAC-Based VLAN Configuration

## Introduction to MAC-Based VLAN

MAC-based VLANs group VLAN members by MAC address. They only apply to untagged frames.

When receiving an untagged frame, the device looks up the list of MAC-to-VLAN mappings based on the MAC address of the frame for a match. If a match is found, the system forwards the frame in the corresponding VLAN. If no match is found, the system looks up other types of VLANs to make the forwarding decision.

MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

## Approaches to Creating MAC Address-to-VLAN Mappings

In addition to creating MAC address-to-VLAN mappings at the CLI, you can use an authentication server to automatically issue MAC address-to-VLAN mappings.

- Manually Static configuration (through CLI)

You can associate MAC addresses with VLANs by using corresponding commands.

- Automatic configuration through the authentication server (that is, VLAN issuing)

The device associates MAC addresses with VLANs dynamically based on the information provided by the authentication server. If a user goes offline, the corresponding MAC address-to-VLAN association is removed automatically. Automatic configuration requires MAC address-to–VLAN mapping be configured on the authentication server. For detailed information, refer to *802.1X Configuration* in the *Security Volume*.

The two configuration approaches can be used at the same time, that is, you can configure a MAC address-to-VLAN entry on both the local device and the authentication server at the same time. Note that the MAC address-to-VLAN entry configuration takes effect only when the configuration on the local device is consistent with that on the authentication server. Otherwise, the previous configuration takes effect.

## Configuring a MAC Address-Based VLAN

**Note**

MAC-based VLANs are available only on hybrid ports.

Follow these steps to configure a MAC-based VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Associate MAC addresses with a VLAN | **mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [ **priority** *priority* ] | Required |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter Ethernet interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Use either command.<br>In Ethernet interface view, the subsequent configurations apply only to the current port; in port group view, the subsequent configurations apply to all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the link type of the port(s) as hybrid | | **port link-type hybrid** | Required |
| Configure the current hybrid port(s) to permit packets of specific MAC-based VLANs to pass through | | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required<br>By default, a hybrid port only permits the packets of VLAN 1 to pass through. |
| Enable MAC-based VLAN | | **mac-vlan enable** | Required<br>Disabled by default |
| Configure VLAN matching precedence | | **vlan precedence** { **mac-vlan** \| **ip-subnet-vlan** } | Optional<br>By default, VLANs are preferentially matched based on MAC addresses. |

# Protocol-Based VLAN Configuration

## Introduction to Protocol-Based VLAN

**Note**

Protocol-based VLANs are only applicable on hybrid ports.

In this approach, inbound packets are assigned to different VLANs based on their protocol types and encapsulation formats. The protocols that can be used for VLAN assignment include IP, IPX, and AppleTalk (AT). The encapsulation formats include Ethernet II, 802.3 raw, 802.2 LLC, and 802.2 SNAP.

A protocol-based VLAN is defined by a protocol template comprised of encapsulation format and protocol type. A port can be associated with multiple protocol templates. An untagged packet reaching a port associated with protocol-based VLANs will be processed as follows.

- If the packet matches a protocol template, the packet will be tagged with the VLAN tag corresponding to the protocol template.
- If the packet matches no protocol template, the packet will be tagged with the default VLAN ID of the port.

The port processes a tagged packet as it processes tagged packets of a port-based VLAN.

- If the port permits the VLAN ID of the packet to pass through, the port forwards the packet.
- If the port does not permit the VLAN ID of the packet to pass through, the port drops the packet.

This feature is mainly used to assign packets of the specific service type to a specific VLAN.

## Configuring a Protocol-Based VLAN

Follow these steps to configure a protocol-based VLAN:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter VLAN view | | **vlan** *vlan-id* | Required<br>If the specified VLAN does not exist, this command creates the VLAN first. |
| Create a protocol template for the VLAN | | **protocol-vlan** [ *protocol-index* ] { **at** \| **ipv4** \| **ipv6** \| **ipx** { **ethernetii** \| **llc** \| **raw** \| **snap** } \| **mode** { **ethernetii etype** *etype-id* \| **llc** { **dsap** *dsap-id* [ **ssap** *ssap-id* ] \| **ssap** *ssap-id* } \| **snap etype** *etype-id* } } | Required |
| Exit VLAN view | | **quit** | Required |
| Enter interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In port group view, the subsequent configurations apply to all ports in the port group.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure the port link type as hybrid | | **port link-type hybrid** | Required |
| Configure current hybrid port(s) to permit the packets of the specified protocol-based VLANs to pass through | | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required |
| Associate the hybrid port(s) with the specified protocol-based VLAN | | **port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [ **to** *protocol-end* ] \| **all** } | Required |

**Caution**

- Do not configure both the *dsap-id* and *ssap-id* arguments in the **protocol-vlan** command as 0xe0 or 0xff when configuring the user-defined template for **llc** encapsulation. Otherwise, the encapsulation format of the matching packets will be the same as that of the **ipx llc** or **ipx raw** packets respectively.
- When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **ethernetii etype** *etype-id* to 0x0800, 0x8137, 0x809b, or 0x86dd. Otherwise, the encapsulation format of the matching packets will be the same as that of the IPv4, IPX, AppleTalk, and IPv6 packets respectively.
- A protocol-based VLAN on a hybrid port can process only untagged inbound packets, whereas the voice VLAN in automatic mode on a hybrid port can process only tagged voice traffic. Therefore, do not configure a VLAN as both a protocol-based VLAN and a voice VLAN. For more information, refer to Voice VLAN Configuration.
- After you configure a command on a Layer-2 aggregate interface, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port.

# IP Subnet-Based VLAN Configuration

## Introduction

In this approach, packets are assigned to VLANs based on their source IP addresses and subnet masks. A port configured with IP subnet-based VLANs assigns a received untagged packet to a VLAN based on the source address of the packet.

This feature is used to assign packets from the specified network segment or IP address to a specific VLAN.

## Configuring an IP Subnet-Based VLAN

**Note**

This feature is only applicable on hybrid ports.

Follow these steps to configure an IP subnet-based VLAN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Associate an IP subnet with the current VLAN | | **ip-subnet-vlan** [ *ip-subnet-index* ] **ip** *ip-address* [ *mask* ] | Required<br>The IP network segment or IP address to be associated with a VLAN cannot be a multicast network segment or a multicast address. |
| Return to system view | | **quit** | — |
| Enter interface view or port group view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use either command.<br>• In Ethernet interface view, the subsequent configurations apply to the current port.<br>• In port group view, the subsequent configurations apply to all ports in the port group.<br>• In Layer-2 aggregate interface view, the subsequent configurations apply to the Layer-2 aggregate interface and all its member ports. |
| | Enter Layer-2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure port link type as hybrid | | **port link-type hybrid** | Required |
| Configure the hybrid port(s) to permit the specified IP subnet-based VLANs to pass through | | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required |
| Associate the hybrid port(s) with the specified IP subnet-based VLAN | | **port hybrid ip-subnet-vlan vlan** *vlan-id* | Required |

**Note**

After you configure a command on a Layer-2 aggregate interface, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port.

# Displaying and Maintaining VLAN

| To do... | Use the command… | Remarks |
|---|---|---|
| Display VLAN information | **display vlan** [ *vlan-id1* [ **to** *vlan-id2* ] \| **all** \| **dynamic** \| **interface** *interface-type interface-number.subnumber* \| **reserved** \| **static** ] | Available in any view |
| Display VLAN interface information | **display interface vlan-interface** [ *vlan-interface-id* ] | Available in any view |
| Display hybrid ports or trunk ports on the device | **display port** { **hybrid** \| **trunk** } | Available in any view |

| To do... | Use the command… | Remarks |
|---|---|---|
| Display MAC address-to-VLAN entries | **display mac-vlan { all** \| **dynamic** \| **mac-address** *mac-address* [ **mask** *mac-mask* ] \| **static** \| **vlan vlan-id }** | Available in any view |
| Display all interfaces with MAC-based VLAN enabled | **display mac-vlan interface** | Available in any view |
| Display protocol information and protocol indexes of the specified VLANs | **display protocol-vlan vlan** { *vlan-id* [ **to** *vlan-id* ] \| **all** } | Available in any view |
| Display protocol-based VLAN information on specified interfaces | **display protocol-vlan interface** { *interface-type interface-number* [ **to** *interface-type interface-number* ] \| **all** } | Available in any view |
| Display IP subnet-based VLAN information and IP subnet indexes of specified VLANs | **display ip-subnet-vlan vlan** { *vlan-id* [ **to** *vlan-id* ] \| **all** } | Available in any view |
| Display the IP subnet-based VLAN information and IP subnet indexes of specified ports | **display ip-subnet-vlan interface** { *interface-list* \| **all** } | Available in any view |
| Clear statistics on a port | **reset counters interface** [ *interface-type* [ *interface-number* ] ] | Available in user view |

**Note**

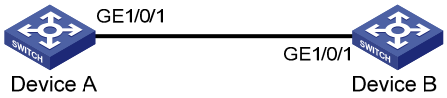
The **reset counters interface** command can be used to clear statistics on a VLAN interface. For more information, refer to *Ethernet Interface Commands* in the *Access Volume*.

# VLAN Configuration Example

## Network requirements

- Device A connects to Device B through a trunk port GigabitEthernet 1/0/1;
- The default VLAN ID of GigabitEthernet 1/0/1 is 100;
- GigabitEthernet 1/0/1 allows packets from VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

**Figure 1-4** Network diagram for port-based VLAN configuration




## Configuration procedure

1) Configure Device A

# Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100.

```
<DeviceA> system-view
```

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 100
[DeviceA-vlan100] vlan 6 to 50
Please wait... Done.
```

# Enter GigabitEthernet 1/0/1 interface view.

```
[DeviceA] interface GigabitEthernet 1/0/1
```

# Configure GigabitEthernet 1/0/1 as a trunk port and configure its default VLAN ID as 100.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

# Configure GigabitEthernet 1/0/1 to deny the packets of VLAN 1 (by default, the packets of VLAN 1 are permitted to pass through on all the ports).

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

# Configure GigabitEthernet 1/0/1 to permit packets from VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 6 to 50 100
Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] quit
```

2) Configure Device B as you configure Device A.

## Verification

Verifying the configuration on Device A is similar to that of Device B. So only Device A is taken for example here.

# Display the information about GigabitEthernet 1/0/1 of Device A to verify the above configurations.

```
<DeviceA> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 001e-c16f-ae68
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 100
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: trunk
  VLAN passing  : 2, 6-50, 100
```

```
 VLAN permitted: 2, 6-50, 100
 Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Peak value of input: 0 bytes/sec, at 2000-04-26 12:01:40
Peak value of output: 0 bytes/sec, at 2000-04-26 12:01:40
Last 300 seconds input:  0 packets/sec 0 bytes/sec      -%
Last 300 seconds output:  0 packets/sec 0 bytes/sec     -%
Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts
Input (normal):  0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

The output above shows that:

- The port (GigabitEthernet 1/0/1) is a trunk port.
- The default VLAN of the port is VLAN 100.
- The port permits packets of VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

Therefore, the configuration is successful.

# 2 Isolate-User-VLAN Configuration

When configuring an isolate-user VLAN, go to these sections for information you are interested in:



## Overview

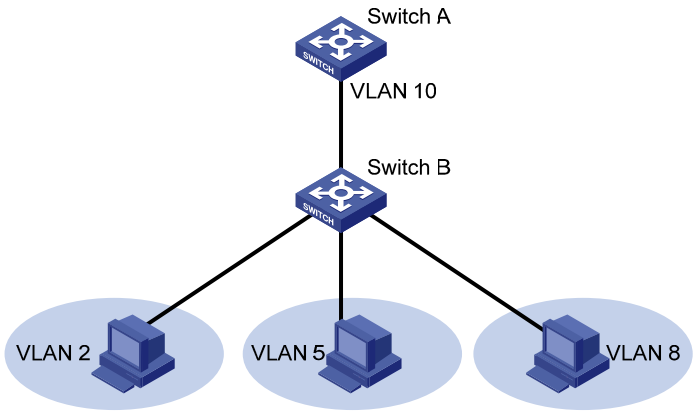
An isolate-user-VLAN adopts a two-tier VLAN structure. In this approach, two types of VLANs, isolate-user-VLAN and secondary VLAN, are configured on the same device.

The following are the characteristics of the isolate-user-VLAN implementation:

- Isolate-user-VLANs are mainly used for upstream data exchange. An isolate-user-VLAN can be associated with multiple secondary VLANs. As the upstream device is aware of only the isolate-user-VLAN but not the secondary VLANs, network configuration is simplified and VLAN resources are saved.
- You can isolate the Layer 2 traffic of different users by assigning the ports connected to them to different secondary VLANs. To enable communication between secondary VLANs associated with the same isolate-user-VLAN, you can enable local proxy ARP on the upstream device to realize Layer 3 communication between the secondary VLANs.

As illustrated in the following figure, the isolate-user-VLAN function is enabled on Switch B. VLAN 10 is the isolate-user-VLAN, and VLAN 2, VLAN 5, and VLAN 8 are secondary VLANs associated with VLAN 10 and are invisible to Switch A.

**Figure 2-1** An isolate-user-VLAN example




## Configuring Isolate-User-VLAN

Configure the isolate-user-VLAN through the following steps:

1) Configure the isolate-user-VLAN;
2) Configure the secondary VLANs;

3) Assign non-trunk ports to the isolate-user-VLAN and ensure that at least one port takes the isolate-user-VLAN as its default VLAN;
4) Assign non-trunk ports to each secondary VLAN and ensure that at least one port in a secondary VLAN takes the secondary VLAN as its default VLAN;
5) Associate the isolate-user-VLAN with the specified secondary VLANs.

Follow these steps to configure an isolate-user-VLAN:

| To do... | | Use the command | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a VLAN and enter VLAN view | | **vlan** *vlan-id* | — |
| Configure the VLAN as an isolate-user-VLAN | | **isolate-user-vlan enable** | Required |
| Return to system view | | **quit** | — |
| Assign ports to the isolate-user-VLAN and ensure that at least one port takes the isolate-user-VLAN as its default VLAN | Access port | Refer to Assigning an Access Port to a VLAN | Use either approach. |
| | Hybrid port | Refer to Assigning a Hybrid Port to a VLAN | |
| Return to system view | | **quit** | — |
| Create secondary VLANs | | **vlan** { *vlan-id1* [ **to** *vlan-id2* ] \| **all** } | Required |
| Quit to system view | | **quit** | — |
| Assign ports to each secondary VLAN and ensure that at least one port in a secondary VLAN takes the secondary VLAN as its default VLAN | Access port | Refer to Assigning an Access Port to a VLAN | Required to choose either |
| | Hybrid port | Refer to Assigning a Hybrid Port to a VLAN | |
| Return to system view | | **quit** | — |
| Associate the isolate-user-VLAN with the specified secondary VLANs | | **isolate-user-vlan** *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [ **to** *secondary-vlan-id* ] | Required |

**Note**

After associating an isolate-user-VLAN with the specified secondary VLANs, you cannot add/remove a port to/from each involved VLAN or remove each involved VLAN. To do that, you must cancel the association first.

# Displaying and Maintaining Isolate-User-VLAN

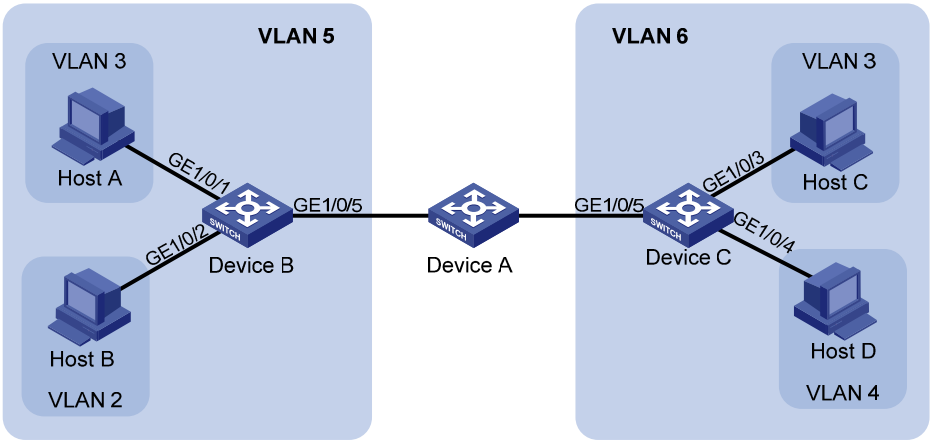
| To do... | Use the command... | Remarks |
|---|---|---|
| Display the mapping between an isolate-user-VLAN and its secondary VLAN(s) | **display isolate-user-vlan** [ *isolate-user-vlan-id* ] | Available in any view |

# Isolate-User-VLAN Configuration Example

## Network requirements

- Connect Device A to downstream devices Device B and Device C;
- Configure VLAN 5 on Device B as an isolate-user-VLAN, assign the uplink port GigabitEthernet 1/0/5 to VLAN 5, and associate VLAN 5 with secondary VLANs VLAN 2 and VLAN 3. Assign GigabitEthernet 1/0/2 to VLAN 2 and GigabitEthernet 1/0/1 to VLAN 3.
- Configure VLAN 6 on Device C as an isolate-user-VLAN, assign the uplink port GigabitEthernet 1/0/5 to VLAN 6, and associate VLAN 6 with secondary VLANs VLAN 3 and VLAN 4. Assign GigabitEthernet 1/0/3 to VLAN 3 and GigabitEthernet 1/0/4 to VLAN 4.
- For Device A, Device B only has VLAN 5 and Device C only has VLAN 6.

**Figure 2-2** Network diagram for isolate-user-VLAN configuration




## Configuration procedure

The following part provides only the configuration on Device B and Device C.

1) Configure Device B

# Configure the isolate-user-VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] port gigabitethernet 1/0/5
[DeviceB-vlan5] quit
```

# Configure the secondary VLANs.

```
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/1
[DeviceB-vlan3] quit
```

```
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

# Associate the isolate-user-VLAN with the secondary VLANs.

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

2) Configure Device C

# Configure the isolate-user-VLAN.

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] isolate-user-vlan enable
[DeviceC-vlan6] port gigabitethernet 1/0/5
[DeviceC-vlan6] quit
```

# Configure the secondary VLANs.

```
[DeviceC] vlan 3
[DeviceC-vlan3] port gigabitethernet 1/0/3
[DeviceC-vlan3] quit
[DeviceC] vlan 4
[DeviceC-vlan4] port gigabitethernet 1/0/4
```

# Associate the isolate-user-VLAN with the secondary VLANs.

```
[DeviceC-vlan4] quit
[DeviceC] isolate-user-vlan 6 secondary 3 to 4
```

## Verification

# Display the isolate-user-VLAN configuration on Device B.

```
[DeviceB] display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 5
 Secondary VLAN ID : 2-3

 VLAN ID: 5
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged   Ports: none
 Untagged Ports:
    gigabitethernet 1/0/1          gigabitethernet 1/0/2          gigabitethernet 1/0/5

 VLAN ID: 2
 VLAN Type: static
 Isolate-user-VLAN type : secondary
Route Interface: not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports: none
 Untagged Ports:
```

```
   gigabitethernet 1/0/2            gigabitethernet 1/0/5

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
   gigabitethernet 1/0/1            gigabitethernet 1/0/5
```

# 3 Voice VLAN Configuration

When configuring a voice VLAN, go to these sections for information you are interested in:



## Overview

A voice VLAN is configured specially for voice traffic. After assigning the ports connecting to voice devices to a voice VLAN, you can configure quality of service (QoS) parameters for the voice traffic, thus improving transmission priority and ensuring voice quality.

A device determines whether a received packet is a voice packet by checking its source MAC address. A packet whose source MAC address complies with the voice device Organizationally Unique Identifier (OUI) address is regarded as voice traffic and assigned to the voice VLAN.

You can configure the OUI addresses in advance or use the default OUI addresses. Table 3-1 lists the default OUI address for each vendor's devices.

**Table 3-1** The default OUI addresses of different vendors

| Number | OUI address | Vendor |
|---|---|---|
| 1 | 0001-e300-0000 | Siemens phone |
| 2 | 0003-6b00-0000 | Cisco phone |
| 3 | 0004-0d00-0000 | Avaya phone |
| 4 | 00d0-1e00-0000 | Pingtel phone |
| 5 | 0060-b900-0000 | Philips/NEC phone |
| 6 | 00e0-7500-0000 | Polycom phone |
| 7 | 00e0-bb00-0000 | 3Com phone |

**Note**

- In general, as the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE. OUI addresses mentioned in this document, however, are different from those in common sense. OUI addresses in this document are used by the system to determine whether a received packet is a voice packet. They are the results of the AND operation of the two arguments *mac-address* and *oui-mask* in the **voice vlan mac-address** command.
- You can remove the default OUI address of a device manually and then add new ones manually.

## Voice VLAN Assignment Modes

A port can be assigned to a voice VLAN in one of the following two modes:

- In automatic mode, the system matches the source MAC addresses in the untagged packets sent when the IP phone is powered on against the OUI addresses. If a match is found, the system automatically assigns the port to the voice VLAN, issues ACL rules and configures the packet precedence. You can configure voice VLAN aging time on the device. The system will remove a port from the voice VLAN if no packet is received from the port after the aging time expires. Assigning/removing ports to/from a voice VLAN are automatically performed by the system.
- In manual mode, you should assign an IP phone connecting port to a voice VLAN manually. Then, the system matches the source MAC addresses in the packets against the OUI addresses. If a match is found, the system issues ACL rules and configures the packet precedence. In this mode, assigning/removing ports to/from a voice VLAN are performed manually.
- Both modes forward tagged packets according to their tags.

The following table lists the co-relation between the port voice VLAN mode, the voice traffic type of an IP phone, and the port link type.

**Table 3-2** Co-relation

| Voice VLAN assignment mode | Voice traffic type | Port link type |
|---|---|---|
| Automatic mode | Tagged voice traffic | Access: not supported |
| | | Trunk: supported if the default VLAN of the connecting port exists and is not the voice VLAN and the connecting port belongs to the default VLAN |
| | | Hybrid: supported if the default VLAN of the connecting port exists and is not the voice VLAN and the traffic of the default VLAN is permitted to pass through the connecting port |
| | Untagged voice traffic | Access, Trunk, hybrid: not supported |
| Manual mode | Tagged voice traffic | Access: not supported |
| | | Trunk: supported if the default VLAN of the connecting port exists and is not the voice VLAN and the connecting port belongs to the default VLAN |
| | | Hybrid: supported if the default VLAN of the connecting port exists and is not the voice VLAN, the traffice of the default VLAN is permitted to pass through the port, and the traffic of the Voice VLAN is permitted to pass through the connecting port tagged |
| | Untagged voice traffic | Access: supported if the default VLAN of the connecting port is the voice VLAN |
| | | Trunk: supported if the default VLAN of the connecting port is the voice VLAN and that the voice VLAN is permitted to pass through the connecting port |
| | | Hybrid port: supported if the default VLAN of the connecting port is the voice VLAN and is permitted to pass through the connecting port untagged |

**Caution**

If an IP phone sends tagged voice traffic and its connecting port is configured with 802.1X authentication and guest VLAN, you should assign different VLAN IDs for the voice VLAN, the default VLAN of the connecting port, and the 802.1X guest VLAN.

**Note**

- The default VLANs for all ports are VLAN 1. You can configure the default VLAN of a port and configure a port to permit a certain VLAN to pass through with commands. For more information, refer to Port-Based VLAN Configuration.
- Use the **display interface** command to display the default VLAN of a port and the VLANs permitted to pass through the port.

### Security Mode and Normal Mode of Voice VLANs

Voice VLAN-enabled ports can operate in security mode or normal mode based on their inbound packet filtering mechanisms.

- Security mode: only voice packets whose source MAC addresses comply with the recognizable OUI addresses can pass through the voice VLAN-enabled inbound port, while other non-voice packets are dropped, including authentication packets, such as 802.1X authentication packets.
- Normal mode: both voice packets and non-voice packets are allowed to pass through a voice VLAN-enabled inbound port. Voice packets are forwarded according to the voice VLAN forwarding mechanism whereas the non-voice packets are forwarded according to the normal VLAN forwarding mechanism.

It is recommended not to transmit both voice packets and non-voice packets in a voice VLAN. If necessary, please ensure that the voice VLAN security mode is disabled.

## Configuring a Voice VLAN

### Configuration Prerequisites

Before configuring a VLAN as a voice VLAN, create the VLAN first. Note that you cannot configure VLAN 1 (the system-default VLAN) as a voice VLAN.

## Setting a Port to Operate in Automatic Voice VLAN Assignment Mode

Follow these steps to set a port to operate in automatic voice VLAN assignment mode:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the voice VLAN aging time | **voice vlan aging** *minutes* | Optional<br>1440 minutes by default.<br>The voice VLAN aging time configuration is only applicable on ports in automatic voice VLAN assignment mode. |
| Enable the voice VLAN security mode | **voice vlan security enable** | Optional<br>Enabled by default. |
| Add a recognizable OUI address | **voice vlan mac-address** *oui* **mask** *oui-mask* [ **description** *text* ] | Optional<br>By default, each voice VLAN has default OUI addresses configured. Refer to Table 3-1 for the default OUI addresses of different vendors. |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Configure the port to operate in automatic voice VLAN assignment mode | **voice vlan mode auto** | Optional<br>Automatic voice VLAN assignment mode is enabled by default.<br>The voice VLAN assignment modes on different ports are independent of one another. |
| Enable voice VLAN on the port | **voice vlan** *vlan-id* **enable** | Required<br>Not enabled by default |

**Note**

- An 4500G switch supports up to eight voice VLANs globally.
- A protocol-based VLAN on a hybrid port can process only untagged inbound packets, whereas the voice VLAN in automatic mode on a hybrid port can process only tagged voice traffic. Therefore, do not configure a VLAN as both a protocol-based VLAN and a voice VLAN. For more information, refer to Protocol-Based VLAN Configuration.
- Do not configure the default VLAN of a port in automatic voice VLAN assignment mode as the voice VLAN.

## Setting a Port to Operate in Manual Voice VLAN Assignment Mode

Follow these steps to set a port to operate in manual voice VLAN assignment mode:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the voice VLAN security mode | **voice vlan security enable** | Optional<br>Enabled by default. |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Add a recognizable OUI address | | **voice vlan mac-address** *oui* **mask** *oui-mask* [ **description** *text* ] | Optional<br>By default, each voice VLAN has default OUI addresses configured. Refer to Table 3-1 for the default OUI addresses of different vendors. |
| Enter interface view | | **interface** *interface-type interface-number* | — |
| Configure the port to operate in manual voice VLAN assignment mode | | **undo voice vlan mode auto** | Required<br>Disabled by default |
| Assign the port in manual voice VLAN assignment mode to the voice VLAN | Access port | Refer to Assigning an Access Port to a VLAN. | Use one of the three approaches.<br>After you assign an access port to the voice VLAN, the voice VLAN becomes the default VLAN of the port automatically. |
| | Trunk port | Refer to Assigning a Trunk Port to a VLAN. | |
| | Hybrid port | Refer to Assigning a Hybrid Port to a VLAN. | |
| Configure the voice VLAN as the default VLAN of the port | Trunk port | Refer to section Assigning a Trunk Port to a VLAN. | Optional<br>This operation is required for untagged inbound voice traffic and prohibited for tagged inbound voice traffic. |
| | Hybrid port | Refer to Assigning a Hybrid Port to a VLAN. | |
| Enable voice VLAN on the port | | **voice vlan enable** | Required |

**Note**

- An 4500G switch supports up to eight voice VLANs globally.
- You can configure different voice VLANs on different ports at the same time. However, one port can be configured with only one voice VLAN, and this voice VLAN must be a static VLAN that already exists on the device.
- Voice VLAN is mutually exclusive with Link Aggregation Control Protocol (LACP) on a port.
- To make voice VLAN take effect on a port which is enabled with voice VLAN and operates in manual voice VLAN assignment mode, you need to assign the port to the voice VLAN manually.

## Displaying and Maintaining Voice VLAN

| To do... | Use the command... | Remarks |
|---|---|---|
| Display the voice VLAN state | **display voice vlan state** | Available in any view |
| Display the OUI addresses currently supported by system | **display voice vlan oui** | Available in any view |

# Voice VLAN Configuration Examples

## Automatic Voice VLAN Mode Configuration Example

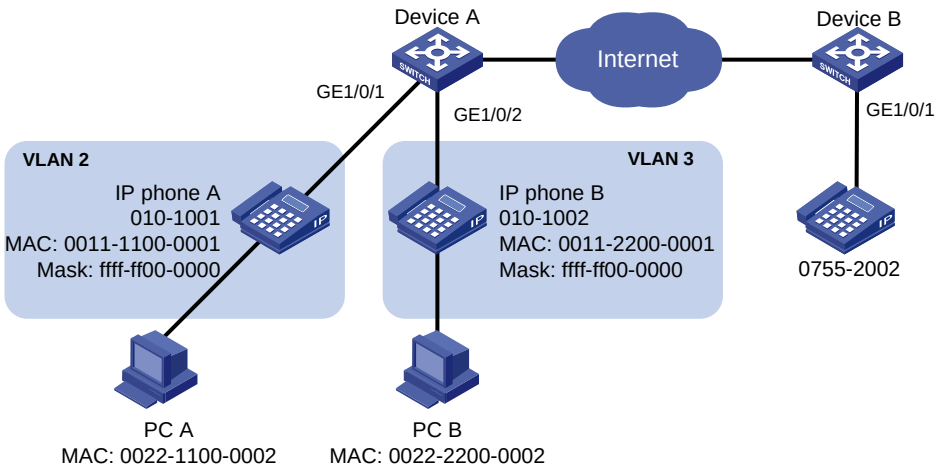
### Network requirements

As shown in Figure 3-1,

- The MAC address of IP phone A is 0011-1100-0001. The phone connects to a downstream device named PC A whose MAC address is 0022-1100-0002 and to GigabitEthernet 1/0/1 on an upstream device named Device A.
- The MAC address of IP phone B is 0011-2200-0001. The phone connects to a downstream device named PC B whose MAC address is 0022-2200-0002 and to GigabitEthernet 1/0/2 on Device A.
- Device A uses voice VLAN 2 to transmit voice packets for IP phone A and voice VLAN 3 to transmit voice packets for IP phone B.

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to work in automatic voice VLAN assignment mode. In addition, if one of them has not received any voice packet in 30 minutes, the port is removed from the corresponding voice VLAN automatically.

**Figure 3-1** Network diagram for automatic voice VLAN assignment mode configuration




### Configuration procedure

# Create VLAN 2 and VLAN 3.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

# Set the voice VLAN aging time to 30 minutes.

```
[DeviceA] voice vlan aging 30
```

# Since GigabitEthernet 1/0/1 may receive both voice traffic and data traffic at the same time, to ensure the quality of voice packets and effective bandwidth use, configure voice VLANs to work in security mode, that is, configure the voice VLANs to transmit only voice packets. (Optional. By default, voice VLANs work in security mode.)

```
[DeviceA] voice vlan security enable
```

# Configure the allowed OUI addresses as MAC addresses prefixed by 0011-1100-0000 or 0011-2200-0000. In this way, Device A identifies packets whose MAC addresses match any of the configured OUI addresses as voice packets.

```
[DeviceA] voice vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
[DeviceA] voice vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
```

# Configure GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode. (Optional. By default, a port operates in automatic voice VLAN assignment mode.)

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

# Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

# Configure VLAN 2 as the voice VLAN for GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] voice vlan mode auto
[DeviceA-GigabitEthernet1/0/2] port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
[DeviceA-GigabitEthernet1/0/2] voice vlan 3 enable
```

## Verification

# Display the OUI addresses, OUI address masks, and description strings supported currently.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-1100-0000  ffff-ff00-0000  IP phone A
0011-2200-0000  ffff-ff00-0000  IP phone B
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

# Display the current states of voice VLANs.

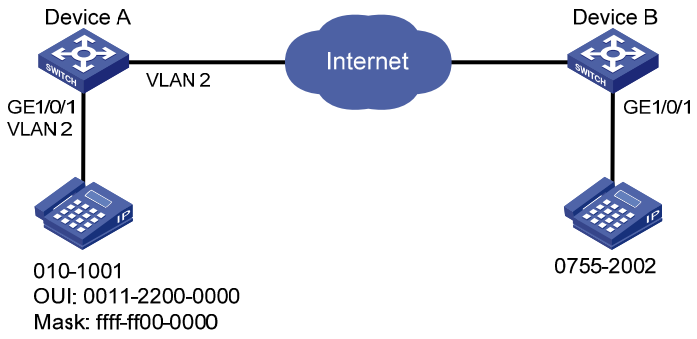
```
<DeviceA> display voice vlan state
Maximum of Voice VLANs: 16
 Current Voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE
 ---------------------------------------------
 GigabitEthernet1/0/1        2           AUTO
 GigabitEthernet1/0/2        3           AUTO
```

## Manual Voice VLAN Assignment Mode Configuration Example

### Network requirements

- Create VLAN 2 and configure it as a voice VLAN permitting only voice traffic to pass through.
- The IP phones send untagged voice traffic. Configure GigabitEthernet 1/0/1 as a hybrid port.
- Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode. Configure GigabitEthernet 1/0/1 to allow voice traffic with an OUI address of 0011-2200-0000, a mask of ffff-ff00-0000, and a description string **test** to be forwarded through the voice VLAN.

**Figure 3-2** Network diagram for manual voice VLAN assignment mode configuration




### Configuration procedure

# Configure the voice VLAN to operate in security mode. (Optional. A voice VLAN operates in security mode by default.)

```
<DeviceA> system-view
[DeviceA] voice vlan security enable
```

# Add a recognizable OUI address 0011-2200-0000.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

# Create VLAN 2 and configure it as the voice VLAN.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] voice vlan 2 enable
```

# Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice vlan mode auto
```

# Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1]port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/1]port link-type hybrid
```

# Configure the voice VLAN (VLAN 2) as the default VLAN of GigabitEthernet 1/0/1 and configure GigabitEthernet 1/0/1 to permit the voice traffic of VLAN 2 to pass through untagged.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

# Enable voice VLAN on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
```

## Verification

# Display the OUI addresses, OUI address masks, and description strings supported currently.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0011-2200-0000  ffff-ff00-0000  test
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

# Display the current voice VLAN state.

```
<DeviceA> display voice vlan state
Maximum of Voice VLANs: 16
 Current Voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 100 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE
 ---------------------------------------------
 GigabitEthernet1/0/1        2           MANUAL
```

# Table of Contents

# 1 GVRP Configuration

The GARP VLAN Registration Protocol (GVRP) is a GARP application. It functions based on the operating mechanism of GARP to maintain and propagate dynamic VLAN registration information for the GVRP devices on the network.

When configuring GVRP, go to these sections for information you are interested in:



## Introduction to GVRP

### GARP

The Generic Attribute Registration Protocol (GARP) provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a LAN the attributes specific to the GARP application, such as the VLAN or multicast address attribute.

GARP itself does not exist on a device as an entity. GARP-compliant participants are known as GARP applications. One example is GVRP. When a GARP participant is present on a port on your device, the port is regarded as a GARP participant.

#### GARP messages and timers

1) GARP messages

A GARP application entity exchanges information with other GARP application entities by:

- Sending Join messages to register with other entities its attributes, the attributes received from other GARP application entities, and the attributes manually configured on it.
- Sending Leave messages to have its attributes deregistered on other devices. A GARP participant also sends Leave messages when it receives Leave messages from other GARP participants or when attributes are manually deregistered on it.
- Sending LeaveAll messages to deregister all the attributes so that all GARP participants can re-register all attributes with each other. A LeaveAll message is sent upon expiration of a LeaveAll timer, which starts upon the startup of a GARP application entity.

Join messages, Leave messages, and LeaveAll message make sure the reregistration and deregistration of GARP attributes are performed in an orderly way.

Through message exchange, all attribute information that needs registration propagates to all GARP participants on the LAN.

2) GARP timers

GARP uses the following four timers to set the interval for sending GARP messages:

- Hold timer — When a GARP application entity receives the first registration request, it starts a Hold timer and collects succeeding requests. When the timer expires, the entity sends all these requests in one Join message. This helps you save bandwidth.
- Join timer — A GARP participant sends a Join message at most twice for reliability sake and uses a Join timer to set the sending interval. If the first Join message has not been acknowledged before the Join timer expires, the GARP participant sends the second Join message.
- Leave timer — Starts upon receipt of a Leave message sent for deregistering some attribute information. If no Join message is received before this timer expires, the GARP participant removes the attribute information as requested.
- LeaveAll timer — Starts when a GARP participant starts. When this timer expires, the entity sends a LeaveAll message so that other participants can re-register its attribute information. Then, a LeaveAll timer starts again.

---

**Note**

- The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.
- On a GARP-enabled network, a device may send LeaveAll messages at the interval set by its LeaveAll timer or the LeaveAll timer on another device on the network, whichever is smaller. This is because each time a device on the network receives a LeaveAll message it resets its LeaveAll timer.

---

## Operating mechanism of GARP

The GARP mechanism allows the configuration of a GARP application entity to propagate throughout a LAN quickly. In GARP, a GARP application entity registers or deregisters its attributes with other entities by making or withdrawing declarations of attributes and at the same time, based on received declarations or withdrawals, handles attributes of other entities. When a port receives an attribute declaration, it registers the attribute; when a port receives an attribute withdrawal, it deregisters the attribute.

GARP application entities send protocol data units (PDUs) with a particular multicast MAC address as destination. Based on this address, a device can identify to which GVRP application (GVRP for example) a GARP PDU will be delivered.

### GARP message format

**Figure 1-1** GARP message format

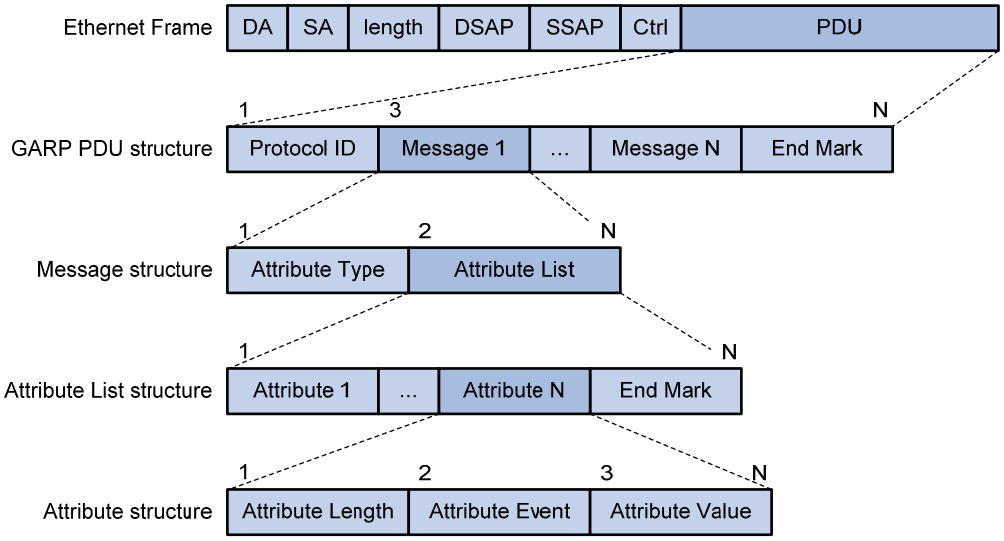



Figure 1-1 illustrates the GARP message format. Table 1-1 describes the GARP message fields.

**Table 1-1** Description on the GARP message fields

| Field | Description | Value |
|---|---|---|
| Protocol ID | Protocol identifier for GARP | 1 |
| Message | One or multiple messages, each containing an attribute type and an attribute list | — |
| Attribute Type | Defined by the concerned GARP application | 0x01 for GVRP, indicating the VLAN ID attribute |
| Attribute List | Contains one or multiple attributes | — |
| Attribute | Consists of an Attribute Length, an Attribute Event, and an Attribute Value | — |
| Attribute Length | Number of octets occupied by an attribute, inclusive of the attribute length field | 2 to 255 (in bytes) |
| Attribute Event | Event described by the attribute | • 0: LeaveAll event<br>• 1: JoinEmpty event<br>• 2: JoinIn event<br>• 3: LeaveEmpty event<br>• 4: LeaveIn event<br>• 5: Empty event |
| Attribute Value | Attribute value | VLAN ID for GVRP<br>If the Attribute Event is LeaveAll, Attribute Value is omitted. |
| End Mark | Indicates the end of a GARP PDU | 0x00 |

## GVRP

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices to its local database

about active VLAN members and through which port they can be reached. It thus ensures that all GVRP participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP provides the following three registration types on a port:

- Normal — Enables the port to dynamically register and deregister VLANs, and to propagate both dynamic and static VLAN information.
- Fixed — Disables the port to dynamically register and deregister VLANs or propagate information about dynamic VLANs, but allows the port to propagate information about static VLANs. A trunk port with fixed registration type thus allows only manually configured VLANs to pass through even though it is configured to carry all VLANs.
- Forbidden — Disables the port to dynamically register and deregister VLANs and to propagate VLAN information except information about VLAN 1. A trunk port with forbidden registration type thus allows only VLAN 1 to pass through even though it is configured to carry all VLANs.

### Protocols and Standards

GVRP is described in IEEE 802.1Q.

## GVRP Configuration Task List

Complete these tasks to configure GVRP:

| Task | Remarks |
|---|---|
| Configuring GVRP Functions | Required |
| Configuring GARP Timers | Optional |

**Note**

- GVRP configuration made in Ethernet interface view or Layer-2 aggregate interface view takes effect on the current interface only; .GVRP configuration made in port group view takes effect on all the member ports in the group.
- GVRP configuration made on a member port in an aggregation group takes effect only after the port is removed from the aggregation group.

## Configuring GVRP Functions

Before enabling GVRP on a port, you must enable GVRP globally.

Follow these steps to configure GVRP functions on a trunk port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable GVRP globally | **gvrp** | Required<br>Globally disabled by default. |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter Ethernet interface view, Layer 2 aggregate interface view, or port-group view | Enter Ethernet interface view or Layer 2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Perform either of the commands. |
| | Enter port-group view | **port-group manual** *port-group-name* | |
| Enable GVRP on the port or port group | | **gvrp** | Required<br>Disabled by default. |
| Configure the GVRP registration mode on the port or port group | | **gvrp registration** { **fixed** \| **forbidden** \| **normal** } | Optional<br>The default is **normal**. |

**Note**

- GVRP can be configured only on trunk ports.
- GVRP is mutually exclusive with service loopback.
- In an MSTP network, GVRP can run on only the CIST. In addition, blocked ports on the CIST cannot receive/send GVRP packets.
- If both GVRP and remote port mirroring are used, GVRP may register the remote probe VLAN to unexpected ports, resulting in undesired duplicates to be received by the monitor port. For more information about port mirroring, refer to Port Mirroring Configuration in the Access Volume.
- Enabling GVRP on a Layer 2 aggregate interface enables both the aggregate interface and all selected member ports in the corresponding link aggregation group to participate in dynamic VLAN registration and deregistration.
- On a GVRP-enabled trunk port, you need to configure the port trunk permit vlan all command on the port to ensure that the traffic of all dynamically registered VLANs can pass through the port.

## Configuring GARP Timers

Among the four GARP timers, the LeaveAll timer is configured in system view and takes effect on all ports, while the other three are configured on a port basis.

Follow these steps to configure GARP timers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the GARP LeaveAll timer | **garp timer leaveall** *timer-value* | Optional<br>The default is 1000 centiseconds. |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter Ethernet interface view, Layer 2 aggregate interface view, or port-group view | Enter Ethernet or Layer 2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Perform either of the commands.<br>Depending on the view you accessed, the subsequent configuration takes effect on a port or all ports in a port-group. |
| | Enter port-group view | **port-group manual** *port-group-name* | |
| Configure the Hold timer | | **garp timer hold** *timer-value* | Optional<br>10 centiseconds by default. |
| Configure the Join timer | | **garp timer join** *timer-value* | Optional<br>20 centiseconds by default. |
| Configure the Leave timer | | **garp timer leave** *timer-value* | Optional<br>60 centiseconds by default. |

**Note**

As shown in Table 1-2, the values of GARP timers are dependent on each other:

- If you want to set a value beyond the value range for a timer, you may change the value range by tuning the value of another related timer.
- If you want to restore the default settings of the timers, restore the Hold timer first, and then the Join, Leave, and LeaveAll timers.

**Table 1-2** Dependencies of GARP timers

| Timer | Lower limit | Upper limit |
|---|---|---|
| Hold | 10 centiseconds | No greater than half of the Join timer setting |
| Join | No less than two times the Hold timer setting | Less than half of the leave timer setting |
| Leave | Greater than two times the Join timer setting | Less than the LeaveAll timer setting |
| LeaveAll | Greater than the Leave timer setting | 32765 centiseconds |

## Displaying and Maintaining GVRP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display statistics about GARP | **display garp statistics** [ **interface** *interface-list* ] | Available in any view |
| Display GARP timers for specified or all ports | **display garp timer** [ **interface** *interface-list* ] | Available in any view |
| Display the local VLAN information maintained by GVRP | **display gvrp local-vlan interface** *interface-type interface-number* | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current GVRP state | **display gvrp state interface** *interface-type interface-number* **vlan** *vlan-id* | Available in any view |
| Display statistics about GVRP | **display gvrp statistics** [ **interface** *interface-list* ] | Available in any view |
| Display the global GVRP state | **display gvrp status** | Available in any view |
| Display the information about dynamic VLAN operations performed on a port | **display gvrp vlan-operation interface** *interface-type interface-number* | Available in any view |
| Clear the GARP statistics | **reset garp statistics** [ **interface** *interface-list* ] | Available in user view |

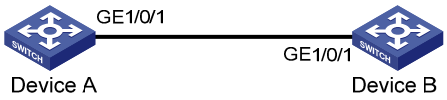
# GVRP Configuration Examples

## GVRP Configuration Example I

### Network requirements

Configure GVRP for dynamic VLAN information registration and update among devices, adopting the normal registration mode on ports.

**Figure 1-2** Network diagram for GVRP configuration




### Configuration procedure

1) Configure Device A

# Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on trunk port GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] quit
```

# Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

# Enable GVRP globally.

```
<DeviceB> system-view
```

```
[DeviceB] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on trunk port GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

# Create VLAN 3 (a static VLAN).

```
[DeviceB] vlan 3
```

3) Verify the configuration

# Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  3
```

# Display dynamic VLAN information on Device B.

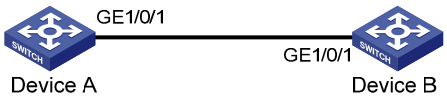
```
[DeviceB] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  2
```

## GVRP Configuration Example II

### Network requirements

Configure GVRP for dynamic VLAN information registration and update among devices. Specify fixed GVRP registration on Device A and normal GVRP registration on Device B.

**Figure 1-3** Network diagram for GVRP configuration




### Configuration procedure

1) Configure Device A

# Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 1/0/1 and set the GVRP registration type to fixed on the port.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] gvrp registration fixed
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

# Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

# Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

# Create VLAN 3 (a static VLAN).

```
[Sysname] vlan 3
```

3) Verify the configuration

# Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 No dynamic vlans exist!
```

# Display dynamic VLAN information on Device B.

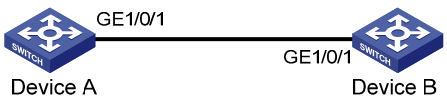
```
[DeviceB] display vlan dynamic
 Now, the following dynamic VLAN exist(s):
  2
```

## GVRP Configuration Example III

### Network requirements

To prevent dynamic VLAN information registration and update among devices, set the GVRP registration mode to **forbidden** on Device A and **normal** on Device B.

**Figure 1-4** Network diagram for GVRP configuration




### Configuration procedure

1) Configure Device A

# Enable GVRP globally.

```
<DeviceA> system-view
[DeviceA] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 1/0/1 and set the GVRP registration type to forbidden on the port.

```
[DeviceA-GigabitEthernet1/0/1] gvrp
[DeviceA-GigabitEthernet1/0/1] gvrp registration forbidden
[DeviceA-GigabitEthernet1/0/1] quit
```

# Create VLAN 2 (a static VLAN).

```
[DeviceA] vlan 2
```

2) Configure Device B

# Enable GVRP globally.

```
<DeviceB> system-view
[DeviceB] gvrp
```

# Configure port GigabitEthernet 1/0/1 as a trunk port, allowing all VLANs to pass through.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] gvrp
[DeviceB-GigabitEthernet1/0/1] quit
```

# Create VLAN 3 (a static VLAN).

```
[DeviceB] vlan 3
```

3) Verify the configuration

# Display dynamic VLAN information on Device A.

```
[DeviceA] display vlan dynamic
 No dynamic vlans exist!
```

# Display dynamic VLAN information on Device B.

```
[DeviceB] display vlan dynamic
 No dynamic vlans exist!
```

# Table of Contents

# 1 QinQ Configuration

When configuring QinQ, go to these sections for information you are interested in:



**Note**

Throughout this document, customer network VLANs (CVLANs), also called inner VLANs, refer to the VLANs that a customer uses on the private network; and service provider network VLANs (SVLANs), also called outer VLANs, refer to the VLANs that a service provider uses to carry VLAN tagged traffic for customers.

## Introduction to QinQ

### Background

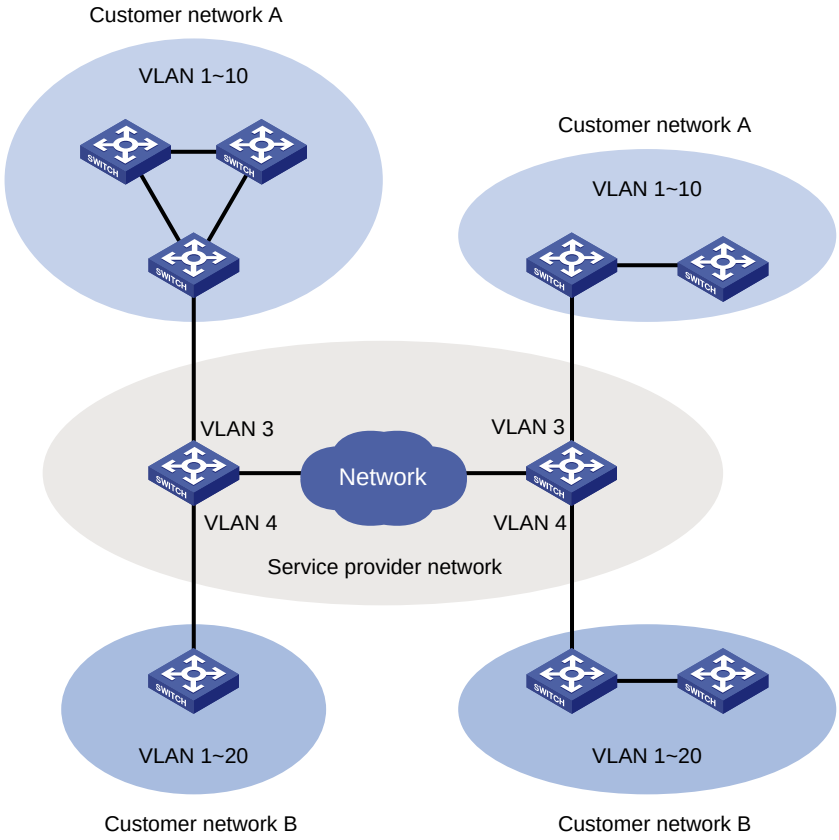
In the VLAN tag field defined in IEEE 802.1Q, only 12 bits are used for VLAN IDs, so a device can support a maximum of 4094 VLANs. In actual applications, however, a large number of VLANs are required to isolate users, especially in metropolitan area networks (MANs), and 4094 VLANs are far from satisfying such requirements.

### QinQ Mechanism and Benefits

The QinQ feature is a flexible, easy-to-implement Layer 2 VPN technique. It enables the edge device on the service provider network to encapsulate an outer VLAN tag in Ethernet frames from customer networks (private networks), so that the Ethernet frames will travel across the service provider network (public network) with double VLAN tags. QinQ enables a service provider to use a single SVLAN to serve customers who have multiple CVLANs.

The devices in the public network forward a frame only according to its outer VLAN tag and learn its source MAC address into the MAC address table of the outer VLAN. The inner VLAN tag of the frame is transmitted as the payload.

**Figure 1-1** Schematic diagram of the QinQ feature




As shown in Figure 1-1, customer network A has CVLANs 1 through 10, while customer network B has CVLANs 1 through 20. The SVLAN allocated by the service provider for customer network A is SVLAN 3, and that for customer network B is SVLAN 4. When a tagged Ethernet frame of customer network A enters the service provider network, it is tagged with outer VLAN 3; when a tagged Ethernet frame of customer network B enters the service provider network, it is tagged with outer VLAN 4. In this way, there is no overlap of VLAN IDs among customers, and traffic from different customers does not become mixed.

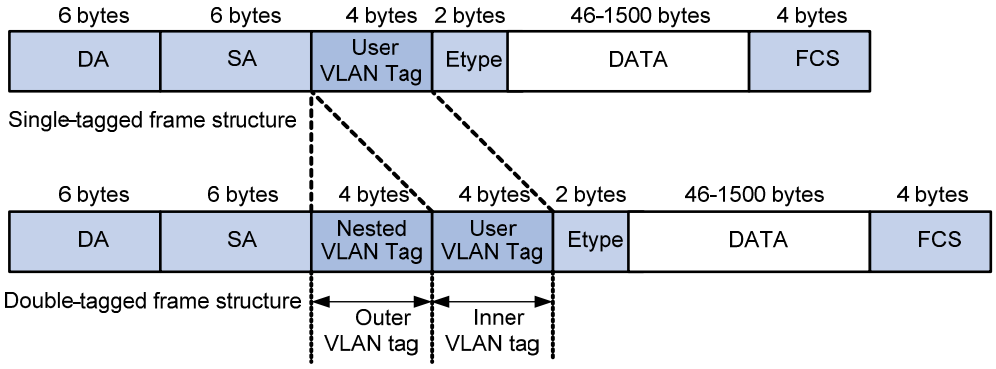
By tagging tagged frames, QinQ expands the available VLAN space from 4094 to 4094 × 4094 and thus satisfies the requirement for VLAN space in MAN. It mainly addresses the following issues:

- Releases the stress on the SVLAN resource.
- Enables customers to plan their CVLANs without conflicting with SVLANs.
- Provides an easy-to-implement Layer 2 VPN solution for small-sized MANs or intranets.

## QinQ Frame Structure

A QinQ frame is transmitted double-tagged over the service provider network. The inner VLAN tag is the CVLAN tag while the outer one is the SVLAN tag that the service provider has allocated to the customer. Figure 1-2 shows the structure of single-tagged and double-tagged Ethernet frames.

**Figure 1-2** Single-tagged frame structure vs. double-tagged Ethernet frame structure




**Note**

The default maximum transmission unit (MTU) of an interface is 1500 bytes. The size of an outer VLAN tag is 4 bytes. Therefore, you are recommended to increase the MTU of each interface on the service provider network. The recommended minimum MTU is 1504 bytes.

## Implementations of QinQ

There are two types of QinQ implementations: basic QinQ and selective QinQ.

1) Basic QinQ

Basic QinQ is a port-based feature. When a frame arrives at a basic QinQ-enabled port, the port tags it with the port's default VLAN tag, regardless of whether the frame is tagged or untagged. If the received frame is already tagged, it becomes a double-tagged frame; if it is untagged, it becomes a frame tagged with the port's default VLAN tag.

2) Selective QinQ

Selective QinQ is a more flexible, VLAN-based implementation of QinQ. In addition to all the functions of basic QinQ, selective QinQ provides per-CVLAN actions for frames received on the same port:

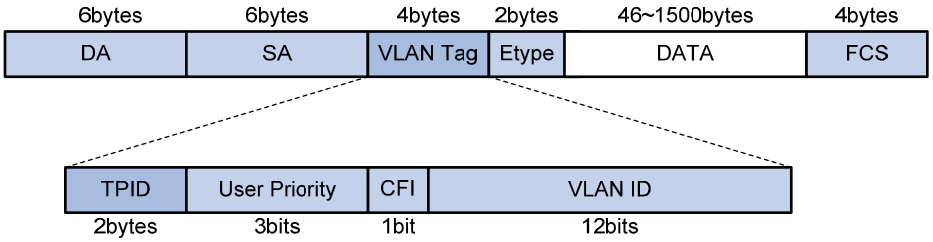
- Tagging frames with different outer VLAN tags based on different inner VLAN IDs.
- Marking the outer VLAN 802.1p priority based on the existing inner VLAN 802.1p priority.
- Modifying the inner VLAN IDs while tagging the frames with outer VLAN tags.

## Modifying the TPID in a VLAN Tag

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The value of this field, as defined in IEEE 802.1Q, is 0x8100.

0 shows the 802.1Q-defined tag structure of an Ethernet frame.

**Figure 1-3** VLAN tag structure of an Ethernet frame




The device determines whether a received frame carries a SVLAN tag or a CVLAN tag by checking the corresponding TPID value. Upon receiving a frame, the device compares the configured TPID value with the value of the TPID field in the frame. If the two match, the devices considers that the frame carries the corresponding VLAN tag. For example, if a frame carries a SVLAN tag with the TPID value 0x9100 and a CVLAN tag with the TPID value 0x8100 while the configured TPID value of the SVLAN tag is 0x9100 and that of the CVLAN tag is 0x8200, the device considers that the frame carries only the SVLAN tag but not the CVLAN tag.

In addition, the systems of different vendors may set the TPID of the outer VLAN tag of QinQ frames to different values. For compatibility with these systems, you can modify the TPID value so that the QinQ frames, when sent to the public network, carry the TPID value identical to the value of a particular vendor to allow interoperability with the devices of that vendor.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling in the network, you cannot set the TPID value to any of the values in the table below.

**Table 1-1** Reserved protocol type values

| Protocol type | Value |
|---|---|
| ARP | 0x0806 |
| PUP | 0x0200 |
| RARP | 0x8035 |
| IP | 0x0800 |
| IPv6 | 0x86DD |
| PPPoE | 0x8863/0x8864 |
| MPLS | 0x8847/0x8848 |
| IPX/SPX | 0x8137 |
| IS-IS | 0x8000 |
| LACP | 0x8809 |
| 802.1x | 0x888E |
| Cluster | 0x88A7 |
| Reserved | 0xFFFD/0xFFFE/0xFFFF |

# QinQ Configuration Task List

**Table 1-2** QinQ configuration task list

| Configuration task | | Remarks |
|---|---|---|
| Configuring Basic QinQ | | Optional |
| Configuring Selective QinQ | Configuring an Outer VLAN Tagging Policy | Optional |
| Configuring the TPID Value in VLAN Tags | | Optional |

**Note**

- QinQ requires configurations only on the service provider network, not on the customer network.
- QinQ configurations made in Ethernet interface view take effect on the current interface only; those made in Layer-2 aggregate interface view take effect on the current aggregate interface and all the member ports in the aggregation group; those made in port group view take effect on all member ports in the current port group.
- Basic and selective QinQ should both be configured on the ports connecting customer networks.
- Do not configure QinQ on a reflector port. For information about reflector ports, refer to *Port Mirroring Configuration* in the *Access Volume*.

# Configuring Basic QinQ

## Enabling Basic QinQ

Follow these steps to enable basic QinQ:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable QinQ on the port(s) | | **qinq enable** | Required<br>Disabled by default. |

# Configuring Selective QinQ

## Configuring an Outer VLAN Tagging Policy

Basic QinQ can only tag received frames with the default VLAN tag of the receiving port, while selective QinQ allows adding different outer VLAN tags based on different inner VLAN tags.

3Com switch 4500G support the configuration of basic QinQ and selective QinQ at the same time on a port and when the two features are both enabled on the port, frames that meet the selective QinQ

condition are handled with selective QinQ on this port first, and the left frames are handled with basic QinQ.

Follow these steps to configure an outer VLAN tagging policy:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter Ethernet or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enter QinQ view and configure the SVLAN tag for the port to add | | **qinq vid** *vlan-id* | Required<br>By default, the SVLAN tag to be added is the default VLAN tag of the receiving port. |
| Tag frames of the specified CVLANs with the current SVLAN | | **raw-vlan-id inbound** { **all** \| *vlan-list* } | Required |

**Caution**

- An inner VLAN tag corresponds to only one outer VLAN tag.
- If you want to change an outer VLAN tag, you must delete the old outer VLAN tag configuration and configure a new outer VLAN tag.

# Configuring the TPID Value in VLAN Tags

You can configure the TPID value in VLAN tags in system view, where the configuration takes effect on all ports of the device.

Follow these steps to configure a TPID value globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the TPID value in the CVLAN tag or the SVLAN tag | **qinq ethernet-type** *hex-value* | Optional<br>By default, the TPID value is 0x8100 |

# QinQ Configuration Examples

## Basic QinQ Configuration Example

### Network requirements

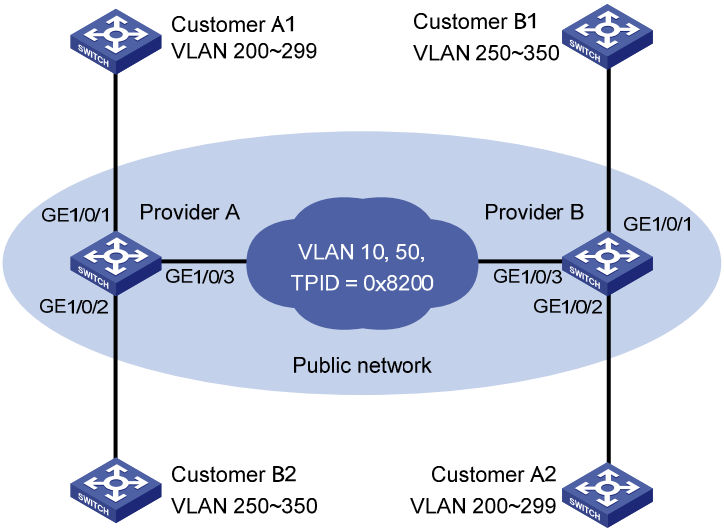
- Provider A and Provider B are edge devices on the service provider network and are interconnected through trunk ports. They belong to SVLAN 10 and 50.

- Customer A1, Customer A2, Customer B1 and Customer B2 are edge devices on the customer network.
- Third-party devices with a TPID value of 0x8200 are deployed between Provider A and Provider B.

Make configuration to achieve the following:

- Frames of VLAN 200 through VLAN 299 can be exchanged between Customer A1and Customer A2 through VLAN 10 of the service provider network.
- Frames of VLAN 250 through VLAN 350 can be exchanged between Customer B1 and Customer B2 through VLAN 50 of the service provider network.

**Figure 1-4** Network diagram for VLAN transparent transmission configuration




## Configuration procedure

**Note**

Make sure that the devices in the service provider network have been configured to allow QinQ packets to pass through.

1) Configuration on Provider A

- Configure GigabitEthernet 1/0/1

# Configure VLAN 10 as the default VLAN of GigabitEthernet 1/0/1.

```
<ProviderA> system-view
[ProviderA] interface gigabitethernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port access vlan 10
```

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
[ProviderA-GigabitEthernet1/0/1] qinq enable
[ProviderA-GigabitEthernet1/0/1] quit
```

- Configure GigabitEthernet 1/0/2

# Configure GigabitEthernet 1/0/2 as a hybrid port and configure VLAN 50 as the default VLAN of the port.

```
[ProviderA] interface gigabitethernet 1/0/2
[ProviderA-GigabitEthernet1/0/2] port link-type hybrid
[ProviderA-GigabitEthernet1/0/2] port hybrid pvid vlan 50
[ProviderA-GigabitEthernet1/0/2] port hybrid vlan 50 untagged
```

# Enable basic QinQ on GigabitEthernet 1/0/2.

```
[ProviderA-GigabitEthernet1/0/2] qinq enable
[ProviderA-GigabitEthernet1/0/2] quit
```

- Configure GigabitEthernet 1/0/3

# Configure GigabitEthernet 1/0/3 as a trunk port to permit frames of VLAN 10 and 50 to pass through.

```
[ProviderA] interface gigabitethernet 1/0/3
[ProviderA-GigabitEthernet1/0/3] port link-type trunk
[ProviderA-GigabitEthernet1/0/3] port trunk permit vlan 10 50
```

# Set the TPID value in the outer tag to 0x8200.

```
[ProviderA-GigabitEthernet1/0/3] quit
[ProviderA] qinq ethernet-type 8200
```

2) Configuration on Provider B

- Configure GigabitEthernet 1/0/1

# Configure VLAN 50 as the default VLAN of GigabitEthernet 1/0/1.

```
<ProviderB> system-view
[ProviderB] interface gigabitethernet 1/0/1
[ProviderB-GigabitEthernet1/0/1] port access vlan 50
```

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
[ProviderB-GigabitEthernet1/0/1] qinq enable
[ProviderB-GigabitEthernet1/0/1] quit
```

- Configure GigabitEthernet 1/0/2

# Configure GigabitEthernet 1/0/2 as a hybrid port and configure VLAN 10 as the default VLAN of the port.

```
[ProviderB] interface gigabitethernet 1/0/2
[ProviderB-GigabitEthernet1/0/2] port link-type hybrid
[ProviderB-GigabitEthernet1/0/2] port hybrid pvid vlan 10
[ProviderB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
```

# Enable basic QinQ on GigabitEthernet 1/0/2.

```
[ProviderB-GigabitEthernet1/0/2] qinq enable
[ProviderB-GigabitEthernet1/0/2] quit
```

- Configure GigabitEthernet 1/0/3

# Configure GigabitEthernet 1/0/3 as a trunk port to permit frames of VLAN 10 and 50 to pass through.

```
[ProviderB] interface gigabitethernet 1/0/3
[ProviderA-GigabitEthernet1/0/B] port link-type trunk
[ProviderA-GigabitEthernet1/0/B] port trunk permit vlan 10 50
```

# Set the TPID value in the outer tag to 0x8200.

```
[ProviderB-GigabitEthernet1/0/3] quit
[ProviderB] qinq ethernet-type 8200
```

3) Configuration on third-party devices

Configure the third-party devices between Provider A and Provider B as follows: configure the port connecting GigabitEthernet 1/0/3 of Provider A and that connecting GigabitEthernet 1/0/3 of Provider B to allow tagged frames of VLAN 10 and 50 to pass through.

## Comprehensive Selective QinQ Configuration Example

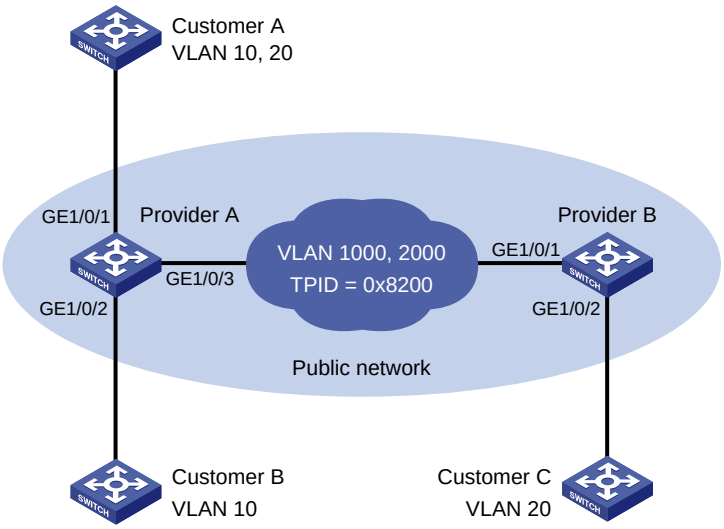
### Network requirements

- Provider A and Provider B are edge devices on the service provider network and are interconnected through trunk ports. They belong to SVLAN 1000 and SVLAN 2000 separately.
- Customer A, Customer B and Customer C are edge devices on the customer network.
- Third-party devices with a TPID value of 0x8200 are deployed between Provider A and Provider B.

Make configuration to achieve the following:

- VLAN 10 frames of Customer A and Customer B can be forwarded to each other across SVLAN 1000;
- VLAN 20 frames of Customer A and Customer C can be forwarded to each other across SVLAN 2000.

**Figure 1-5** Network diagram for comprehensive selective QinQ configuration




### Configuration procedure

**Note**

Make sure that the devices in the service provider network have been configured to allow QinQ packets to pass through.

1) Configuration on Provider A

- Configure GigabitEthernet 1/0/1

# Configure GigabitEthernet 1/0/1 as a hybrid port to permit frames of VLAN 1000 and VLAN 2000 to pass through, and configure GigabitEthernet 1/0/1 to send packets of these VLANs with tags removed.

```
<ProviderA> system-view
```

```
[ProviderA] interface gigabitethernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port link-type hybrid
[ProviderA-GigabitEthernet1/0/1] port hybrid vlan 1000 2000 untagged
```

# Tag CVLAN 10 frames with SVLAN 1000.

```
[ProviderA-GigabitEthernet1/0/1] qinq vid 1000
[ProviderA-GigabitEthernet1/0/1-vid-1000] raw-vlan-id inbound 10
[ProviderA-GigabitEthernet1/0/1-vid-1000] quit
```

# Tag CVLAN 20 frames with SVLAN 2000.

```
[ProviderA-GigabitEthernet1/0/1] qinq vid 2000
[ProviderA-GigabitEthernet1/0/1-vid-2000] raw-vlan-id inbound 20
[ProviderA-GigabitEthernet1/0/1-vid-2000] quit
[ProviderA-GigabitEthernet1/0/1] quit
```

- Configure GigabitEthernet 1/0/2

# Configure GigabitEthernet 1/0/2 as a hybrid port to permit frames of VLAN 1000 to pass through, and configure GigabitEthernet 1/0/2 to send packets of VLAN 1000 with tag removed.

```
[ProviderA] interface gigabitethernet 1/0/2
[ProviderA-GigabitEthernet1/0/2] port link-type hybrid
[ProviderA-GigabitEthernet1/0/2] port hybrid vlan 1000 untagged
```

# Tag CVLAN 10 frames with SVLAN 1000.

```
[ProviderA-GigabitEthernet1/0/2] qinq vid 1000
[ProviderA-GigabitEthernet1/0/2-vid-1000] raw-vlan-id inbound 10
[ProviderA-GigabitEthernet1/0/2-vid-1000] quit
[ProviderA-GigabitEthernet1/0/2] quit
```

- Configure GigabitEthernet 1/0/3

# Configure GigabitEthernet 1/0/3 as a trunk port to permit frames of VLAN 1000 and VLAN 2000 to pass through.

```
[ProviderA] interface gigabitethernet 1/0/3
[ProviderA-GigabitEthernet1/0/3] port link-type trunk
[Sysname-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

# Set the TPID value in the outer tag to 0x8200.

```
[ProviderA-GigabitEthernet1/0/3] quit
[ProviderA] qinq ethernet-type 8200
```

2) Configuration on Provider B

- Configure GigabitEthernet 1/0/1

# Configure GigabitEthernet 1/0/1 as a trunk port to permit frames of VLAN 1000 and VLAN 2000 to pass through.

```
<ProviderB> system-view
[ProviderB] interface gigabitethernet 1/0/1
[ProviderB-GigabitEthernet1/0/1] port link-type trunk
[ProviderB-GigabitEthernet1/0/1] port trunk permit vlan 1000 2000
```

- Configure GigabitEthernet 1/0/2

# Configure GigabitEthernet 1/0/2 as a hybrid port to permit frames of VLAN 2000 to pass through, and configure GigabitEthernet 1/0/2 to send packets of VLAN 2000 with tag removed.

```
[ProviderB] interface gigabitethernet 1/0/2
```

```
[ProviderB-GigabitEthernet1/0/2] port link-type hybrid
[ProviderB-GigabitEthernet1/0/2] port hybrid vlan 2000 untagged
```

# Tag CVLAN 20 frames with SVLAN 2000.

```
[ProviderB-GigabitEthernet1/0/2] qinq vid 2000
[ProviderB-GigabitEthernet1/0/2-vid-2000] raw-vlan-id inbound 20
```

# Set the TPID value in the outer tag to 0x8200.

```
[ProviderA-GigabitEthernet1/0/3] quit
[ProviderA] qinq ethernet-type 8200
```

3) Configuration on third-party devices

Configure the third-party devices between Provider A and Provider B as follows: configure the port connecting GigabitEthernet 1/0/3 of Provider A and that connecting GigabitEthernet 1/0/1 of Provider B to allow tagged frames of VLAN 1000 and VLAN 2000 to pass through.

# Table of Contents

# 1 BPDU Tunneling Configuration

When configuring BPDU tunneling, go to these sections for information you are interested in:



## Introduction to BPDU Tunneling

To avoid loops in your network, you can enable the Spanning Tree Protocol (STP) on your device. Here, the term STP is in a broad sense. It includes STP, RSTP, and MSTP. STP calculates the topology of a network by multicasting bridge protocol data units (BPDUs) at Layer 2. As these BPDUs can be received and processed by all STP-enabled devices, this prevents each network from correctly calculating its independent spanning tree.

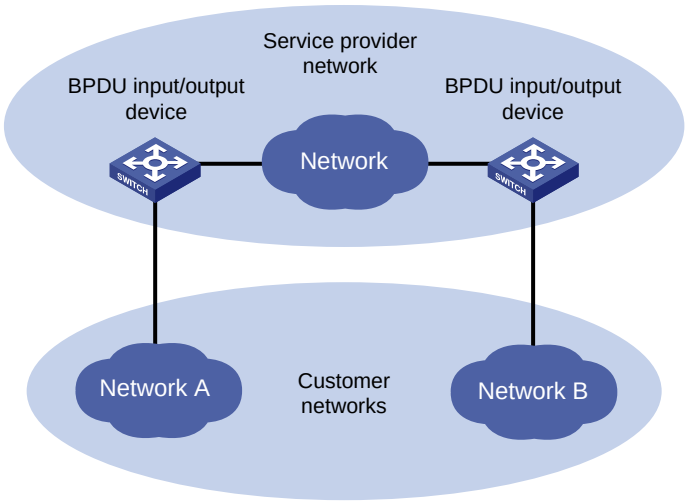
To allow each network to calculate an independent spanning tree with STP, BPDU tunneling was introduced.

BPDU tunneling delivers the following benefits:

- BPDUs can be transmitted transparently. BPDUs of the same customer network can be broadcast in a specific VLAN across the service provider network, so that the geographically dispersed networks of the same customer can implement consistent spanning tree calculation across the service provider network.
- BPDUs of different customer networks can be confined within different VLANs for transmission on the service provider network. Thus, each customer network can perform independent spanning tree calculation.

As shown in Figure 1-1, the upper part is the service provider network, and the lower part represents the customer networks. The customer networks include network A and network B. Enabling the BPDU tunneling function on the edge devices across the service provider network allows BPDUs of the customer networks to be transparently transmitted in the service provider network, and allows each customer network to implement independent spanning tree calculation, without affecting each other.

**Figure 1-1** Network hierarchy of BPDU tunneling




- At the input side of the service provider network, the edge device changes the destination MAC address of a BPDU from a customer network from 0x0180-C200-0000 to a special multicast MAC address, 0x010F-E200-0003 by default. In the service provider's network, the modified BPDUs are forwarded as data packets in the user VLAN.
- At the output side of the service provider network, the edge device recognizes the BPDU with the destination MAC address of 0x010F-E200-0003 and restores its original destination MAC address 0x0180-C200-0000. Then, the device removes the outer VLAN tag, and sends the BPDU to the destination customer network.

**Note**

Make sure, through configuration, that the VLAN tag of the BPDU is neither changed nor removed during its transparent transmission in the service provider network; otherwise, the system will fail to transparently transmit the customer network BPDU correctly.

## Configuring BPDU Transparent Transmission

Perform the following tasks to configure BPDU transparent transmission:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port | Enter Ethernet or Layer-2 aggregate interface view | **interface** *interface-type interface-number* | Required<br>Use either command. |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| group view | Enter port group view | **port-group manual** *port-group-name* | • Settings made in interface view take effect only on the current port.<br>• Settings made in Layer-2 aggregate interface view take effect only on the Layer-2 aggregate interface.<br>• Settings made in port group view take effect on all ports in the port group. |
| Disable STP on the port(s) | | **undo stp enable** | Required |
| Enable BPDU tunneling for STP on the port(s) | | **bpdu-tunnel dot1q stp** | Required<br>By default, BPDU tunneling for STP is disabled. |

# Configuring Destination Multicast MAC Address for BPDU Tunnel Frames

By default, the destination multicast MAC address for BPDU tunnel frames is 0x010F-E200-0003. You can modify it to 0x0100-0CCD-CDD0, 0x0100-0CCD-CDD1 or 0x0100-0CCD-CDD2 through the following configuration.

Follow these steps to configure destination multicast MAC address for BPDU tunnel frames:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the destination multicast MAC address for BPDU tunnel frames | **bpdu-tunnel tunnel-dmac** *mac-address* | Optional<br>0x010F-E200-0003 by default. |

**Note**

For BPDU tunnel frames to be recognized, the destination multicast MAC addresses configured for BPDU tunneling must be the same on the edge devices on the service provider network.

# BPDU Tunneling Configuration Example

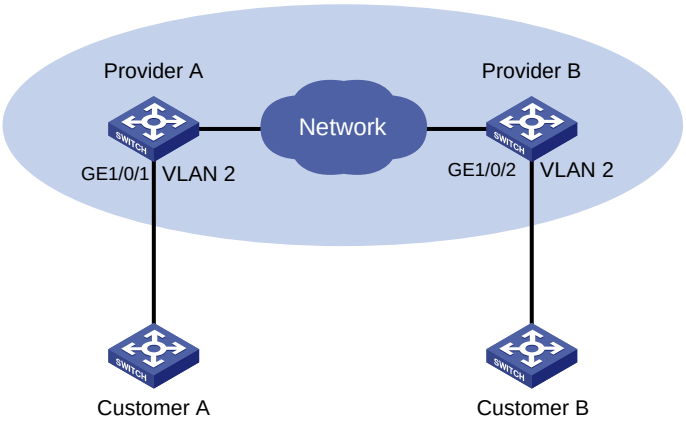
## Network requirements

- Customer A and Customer B are customer network edge devices.
- Provider A and Provider B are service provider network edge devices, which are interconnected through configured trunk ports.

The configuration is required to satisfy the following requirements:

- Geographically dispersed customer network access devices Customer A and Customer B can implement consistent spanning tree calculation across the service provider network.
- The destination multicast MAC address configured for BPDU tunnel frames is 0x0100-0CCD-CDD0.

**Figure 1-2** Network diagram for BPDU tunneling configuration




## Configuration procedure

1) Configuration on Provider A

# Configure the destination multicast MAC address for BPDU tunnel frames as 0x0100-0CCD-CDD0.

```
<ProviderA> system-view
[ProviderA] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

# Configure GigabitEthernet 1/0/1 to transmit packets through VLAN 2.

```
[ProviderA] vlan 2
[ProviderA-vlan2] quit
[ProviderA] interface GigabitEthernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port access vlan 2
```

# Configure GigabitEthernet 1/0/1 to transmit BPDUs transparently.

```
[ProviderA-GigabitEthernet1/0/1] undo stp enable
[ProviderA-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

2) Configuration on Provider B

# Configure the destination multicast MAC address for BPDU tunnel frames as 0x0100-0CCD-CDD0.

```
<ProviderB> system-view
[ProviderB] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

# Configure GigabitEthernet 1/0/2 to transmit packets through VLAN 2.

```
[ProviderB] vlan 2
[ProviderB-vlan2] quit
[ProviderB] interface GigabitEthernet 1/0/2
[ProviderB-GigabitEthernet1/0/2] port access vlan 2
```

# Configure GigabitEthernet 1/0/2 to transmit BPDUs transparently.

```
[ProviderB-GigabitEthernet1/0/2] undo stp enable
```

```
[ProviderB-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
```

# Table of Contents

# 1 Ethernet OAM Configuration

When configuring the Ethernet OAM function, go to these sections for information you are interested in:



## Ethernet OAM Overview

Ethernet OAM (operation, administration, and maintenance) is a tool monitoring Layer-2 link status by sending OAM protocol data units (OAMPDUs) between devices. It helps network administrators manage their networks effectively.

Currently, Ethernet OAM is mainly used to address common link-related issues on the “last mile.” By enabling Ethernet OAM on two devices connected by a point-to-point connection, you can monitor the status of the link. Ethernet OAM provides the following functions:

- Link performance monitoring, for detecting link errors
- Fault detection and alarm, for reporting link errors to the administrators
- Loopback testing, for detecting link errors through non-OAMPDUs

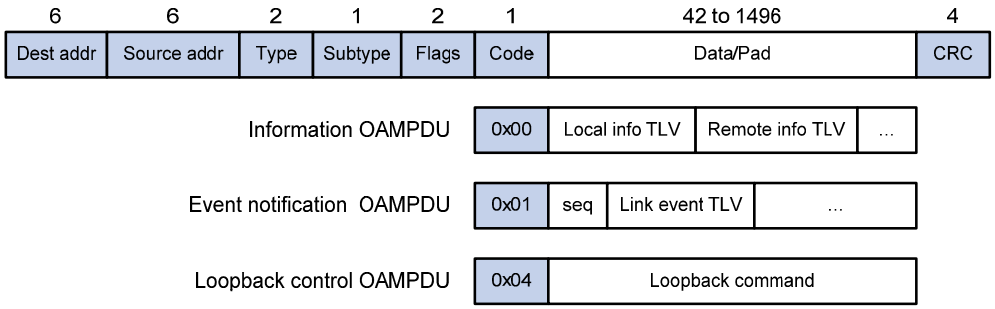
**Note**

Throughout this document, a port with Ethernet OAM enabled is called an Ethernet OAM entity or an OAM entity.

### Types of Ethernet OAMPDUs

Figure 1-1 shows the formats of different types of OAMPDUs.

**Figure 1-1** Formats of different types of Ethernet OAMPDUs




The fields in an OAMPDU are described as follows:

**Table 1-1** Description of the fields in an OAMPDU

| Field | Description |
|---|---|
| Dest addr | Destination MAC address of the Ethernet OAMPDU.<br>It is a slow protocol multicast address 0180c2000002. |
| Source addr | Source MAC address of the Ethernet OAMPDU.<br>It is the bridge MAC address of the sending side and is a unicast MAC address. |
| Type | Type of the encapsulated protocol in the Ethernet OAMPDU.<br>The value is 0x8809. |
| Subtype | The specific protocol being encapsulated in the Ethernet OAMPDU.<br>The value is 0x03. |
| Flags | Status information of an Ethernet OAM entity. |
| Code | Type of the Ethernet OAMPDU |

Table 1-2 shows the function of the three types of OAMPDUs.

**Table 1-2** Functions of different types of OAMPDUs

| OAMPDU type | Function |
|---|---|
| Information OAMPDU | Used for transmitting state information of an Ethernet OAM entity (including the information about the local device and remote devices, and customized information) to the remote Ethernet OAM entity and maintaining OAM connections |
| Event Notification OAMPDU | Used by link monitoring to notify the remote OAM entity when it detects problems on the link in between. |
| Loopback Control OAMPDU | Used for remote loopback control. By inserting the information used to enable/disable loopback to a loopback control OAMPDU, you can enable/disable loopback on a remote OAM entity. |

## Ethernet OAM Implementation

This section describes the working procedures of Ethernet OAM.

### Ethernet OAM connection establishment

Ethernet OAM connection is the base of all the other Ethernet OAM functions. OAM connection establishment is also known as the Discovery phase, where an Ethernet OAM entity discovers remote OAM entities and establishes sessions with them.

In this phase, interconnected OAM entities notify the peer of their OAM configuration information and the OAM capabilities of the local nodes by exchanging Information OAMPDUs and determine whether Ethernet OAM connections can be established. An Ethernet OAM connection can be established only when the settings concerning Loopback, link detecting, and link event of the both sides match. After an Ethernet OAM connection is established, Ethernet OAM takes effect on it.

As for Ethernet OAM connection establishment, a device can operate in active Ethernet OAM mode or passive Ethernet OAM mode. Table 1-3 compares active Ethernet OAM mode with passive Ethernet OAM mode.

**Table 1-3** Active Ethernet OAM mode and passive Ethernet OAM mode

| Item | Active Ethernet OAM mode | Passive Ethernet OAM mode |
|---|---|---|
| Initiating OAM Discovery | Available | Unavailable |
| Responding to OAM Discovery | Available | Available |
| Transmitting Information OAMPDUs | Available | Available |
| Transmitting Event Notification OAMPDUs | Available | Available |
| Transmitting Information OAMPDUs with the Data/Pad field being empty | Available | Available |
| Transmitting Loopback Control OAMPDUs | Available | Unavailable |
| Responding to Loopback Control OAMPDUs | Available (if both sides operate in active OAM mode) | Available |

**Note**

- OAM connections can be initiated only by OAM entities operating in active OAM mode, while those operating in passive mode wait and respond to the connection requests sent by their peers.
- No OAM connection can be established between OAM entities operating in passive OAM mode.

After an Ethernet OAM connection is established, the Ethernet OAM entities on both sides exchange Information OAMPDUs periodically to keep the Ethernet OAM connection valid. If an Ethernet OAM entity receives no Information OAMPDU for five seconds, the Ethernet OAM connection is disconnected.

**Note**

The interval to send Information OAMPDUs is determined by a timer. Up to ten Information OAMPDUs can be sent in a second.

## Link monitoring

Error detection in an Ethernet is difficult, especially when the physical connection in the network is not disconnected but network performance is degrading gradually. Link monitoring is used to detect and indicate link faults in various environments. Ethernet OAM implements link monitoring through the exchange of Event Notification OAMPDUs. Upon detecting a link error event listed in Table 1-4, the local OAM entity sends an Event Notification OAMPDU to notify the remote OAM entity. With the log information, network administrators can keep track of network status in time. Table 1-4 describes the link events.

**Table 1-4** Ethernet OAM link error events

| Ethernet OAM link events | Description |
|---|---|
| Errored symbol event | An errored symbol event occurs when the number of detected symbol errors over a specific detection interval exceeds the predefined threshold. |
| Errored frame event | An errored frame event occurs when the number of detected error frames over a specific interval exceeds the predefined threshold. |
| Errored frame period event | An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the predefined threshold. |
| Errored frame seconds event | When the number of error frame seconds detected on a port over a detection interval reaches the error threshold, an errored frame seconds event occurs. |

**Note**

- The system transforms the period of detecting errored frame period events into the maximum number of 64-byte frames that a port can send in the specific period, that is, the system takes the maximum number of frames sent as the period. The maximum number of frames sent is calculated using this formula: the maximum number of frames = interface bandwidth (bps) × errored frame period event detection period (in ms)/(64 × 8 × 1000)
- If errored frames appear in a certain second, this second is called an errored frame second.

## Remote fault detection

In a network where traffic is interrupted due to device failures or unavailability, the flag field defined in Ethernet OAMPDUs allows an Ethernet OAM entity to send error information to its peer. It can identify the critical link error events listed in Table 1-5.

**Table 1-5** Critical link error events

| Ethernet OAM link events | Description |
|---|---|
| Link Fault | Peer link signal is lost. |
| Dying Gasp | An unexpected fault, such as power failure, occurred. |
| Critical event | An undetermined critical event happened. |

As Information OAMPDUs are exchanged periodically across established OAM connections, an Ethernet OAM entity can inform one of its OAM peers of link faults through Information OAMPDUs. Therefore, the network administrator can keep track of link status in time through the log information and troubleshoot in time.

### Remote loopback testing

Remote loopback testing is available only after the Ethernet OAM connection is established. With remote loopback enabled, the Ethernet OAM entity operating in active Ethernet OAM mode issues remote loopback requests and the peer responds to them. If the peer operates in the loopback mode, it returns all the PDUs except Ethernet OAMPDUs to the senders along the original paths.

Performing remote loopback testing periodically helps to detect network faults in time. Furthermore, performing remote loopback testing by network segments helps to locate network faults.

## Standards and Protocols

Ethernet OAM is defined in IEEE 802.3h.

# Ethernet OAM Configuration Task List

Complete the following tasks to configure Ethernet OAM:

| Task | | Remarks |
|---|---|---|
| Configuring Basic Ethernet OAM Functions | | Required |
| Configuring Link Monitoring | Configuring Errored Symbol Event Detection | Optional |
| | Configuring Errored Frame Event Detection | Optional |
| | Configuring Errored Frame Period Event Detection | Optional |
| | Configuring Errored Frame Seconds Event Detection | Optional |
| Enabling OAM Loopback Testing | | Optional |

# Configuring Basic Ethernet OAM Functions

As for Ethernet OAM connection establishment, a device can operate in active mode or passive mode. After Ethernet OAM is enabled on an Ethernet port, according to its Ethernet OAM mode, the Ethernet port establishes an Ethernet OAM connection with its peer port.

Follow these steps to configure basic Ethernet OAM functions:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **System-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Set Ethernet OAM operating mode | **oam mode** { **active** \| **passive** } | Optional<br>The default is active Ethernet OAM mode. |
| Enable Ethernet OAM on the current port | **oam enable** | Required<br>Ethernet OAM is disabled by default. |

# Configuring Link Monitoring

**Note**

After Ethernet OAM connections are established, the link monitoring periods and thresholds configured in this section take effect on all Ethernet ports automatically.

## Configuring Errored Symbol Event Detection

An errored symbol event occurs when the number of detected symbol errors over a specific detection interval exceeds the predefined threshold.

Follow these steps to configure errored symbol event detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the errored symbol event detection interval | **oam errored-symbol period** *period-value* | Optional<br>1 second by default |
| Configure the errored symbol event triggering threshold | **oam errored-symbol threshold** *threshold-value* | Optional<br>1 by default |

## Configuring Errored Frame Event Detection

An errored frame event occurs when the number of detected error frames over a specific interval exceeds the predefined threshold.

Follow these steps to configure errored frame event detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the errored frame event detection interval | **oam errored-frame period** *period-value* | Optional<br>1 second by default |
| Configure the errored frame event triggering threshold | **oam errored-frame threshold** *threshold-value* | Optional<br>1 by default |

## Configuring Errored Frame Period Event Detection

An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the predefined threshold.

Follow these steps to configure errored frame period event detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the errored frame period event detection period | **oam errored-frame-period period** *period-value* | Optional<br>1000 milliseconds by default |
| Configure the errored frame period event triggering threshold | **oam errored-frame-period threshold** *threshold-value* | Optional<br>1 by default |

## Configuring Errored Frame Seconds Event Detection

An errored frame seconds event occurs when the number of error frame seconds detected on a port over a detection interval exceeds the error threshold.

Follow these steps to configure errored frame seconds event detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the errored frame seconds event detection interval | **oam errored-frame-seconds period** *period-value* | Optional<br>60 second by default |
| Configure the errored frame seconds event triggering threshold | **oam errored-frame-seconds threshold** *threshold-value* | Optional<br>1 by default |

**Caution**

Make sure the errored frame seconds triggering threshold is less than the errored frame seconds detection interval. Otherwise, no errored frame seconds event can be generated.

## Enabling OAM Loopback Testing

Follow these steps to enable Ethernet OAM loopback testing:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **System-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable Ethernet OAM loopback testing | **oam loopback** | Required<br>Disabled by default. |

**Note**

- Ethernet OAM loopback testing is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.
- Loopback testing is available only on full-duplex links that support remote loopback at both ends.
- Ethernet OAM loopback testing needs the support of the peer hardware.
- Enabling Ethernet OAM loopback testing interrupts data communications. After Ethernet OAM loopback testing is disabled, all the ports involved will shut down and then come up. Ethernet OAM loopback testing is disabled when you execute the **undo oam enable** command to disable Ethernet OAM, when you execute the **undo oam loopback** command to disable Ethernet OAM loopback testing, or when the Ethernet OAM connection times out.
- Ethernet OAM loopback testing is only applicable to individual links. It is not applicable to link aggregation member ports. In addition, you cannot assign ports where Ethernet OAM loopback testing is being performed to link aggregation groups. For more information about link aggregation groups, refer to *Link Aggregation Configuration* in the *Access Volume*.
- Enabling internal loopback test on a port in remote loopback test can terminate the remote loopback test. For more information about loopback test, refer to *Ethernet Interface Configuration* in the *Access Volume*.

## Displaying and Maintaining Ethernet OAM Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display global Ethernet OAM configuration | **display oam configuration** | Available in any view |
| Display the statistics on critical events after an Ethernet OAM connection is established | **display oam critical-event** [ **interface** *interface-type interface-number* ] | |
| Display the statistics on Ethernet OAM link error events after an Ethernet OAM connection is established or after you clear the statistics | **display oam link-event** { **local** \| **remote** } [ **interface** *interface-type interface-number* ] | |
| Display the information about an Ethernet OAM connection | **display oam** { **local** \| **remote** } [ **interface** *interface-type interface-number* ] | |

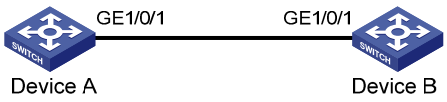
| To do… | Use the command… | Remarks |
|---|---|---|
| Clear statistics on Ethernet OAM packets and Ethernet OAM link error events | **reset oam** [ **interface** *interface-type interface-number* ] | Available in user view only |

# Ethernet OAM Configuration Example

## Network requirements

- Enable Ethernet OAM on Device A and Device B to manage links on data link layer.
- Monitor link performance and collect statistics about the error frames received by Device A.

**Figure 1-2** Network diagram for Ethernet OAM configuration




## Configuration procedure

1) Configure Device A

# Configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode and enable Ethernet OAM for it.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode passivez
[DeviceA-GigabitEthernet1/0/1] oam enable
[DeviceA-GigabitEthernet1/0/1] quit
```

# Set the errored frame detection interval to 20 seconds and set the errored frame event triggering threshold to 10.

```
[DeviceA] oam errored-frame period 20
[DeviceA] oam errored-frame threshold 10
```

2) Configure Device B

# Configure GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode (the default) and enable Ethernet OAM for it.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode active
[DeviceB-GigabitEthernet1/0/1] oam enable
[DeviceB-GigabitEthernet1/0/1] quit
```

3) Verify the configuration

Use the **display oam configuration** command to display the Ethernet OAM configuration. For example:

# Display the Ethernet OAM configuration on Device A.

```
[DeviceA] display oam configuration
Configuration of the link event window/threshold :
```

```
------------------------------------------------------------------------------
Errored-symbol Event period(in seconds)          :     1
Errored-symbol Event threshold                   :     1
Errored-frame Event period(in seconds)           :     20
Errored-frame Event threshold                    :     10
Errored-frame-period Event period(in ms)         :     1000
Errored-frame-period Event threshold             :     1
Errored-frame-seconds Event period(in seconds)   :     60
Errored-frame-seconds Event threshold            :     1
```

Use the **display oam link-event** command to display the statistics about Ethernet OAM link events. For example:

# Display Ethernet OAM link event statistics of the remote end of Device B.

```
[DeviceB] display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
------------------------------------------------------------------------
Event Time Stamp          : 5789        Errored FrameWindow   : 10(100ms)
Errored Frame Threshold   : 1           Errored Frame         : 3
Error Running Total       : 35          Event Running Total   : 17
```

The above information indicates that 35 errors occurred since Ethernet OAM is enabled on Device A, 17 of which are caused by error frames. The link is instable.

# Table of Contents

# 1 Connectivity Fault Detection Configuration

When configuring CFD, go to these sections for information you are interested in:



## Overview

Connectivity Fault Detection (CFD) is an end-to-end per-VLAN link layer Operations, Administration and Maintenance (OAM) mechanism used for link connectivity detection, fault verification, and fault location.

### Basic Concepts in CFD

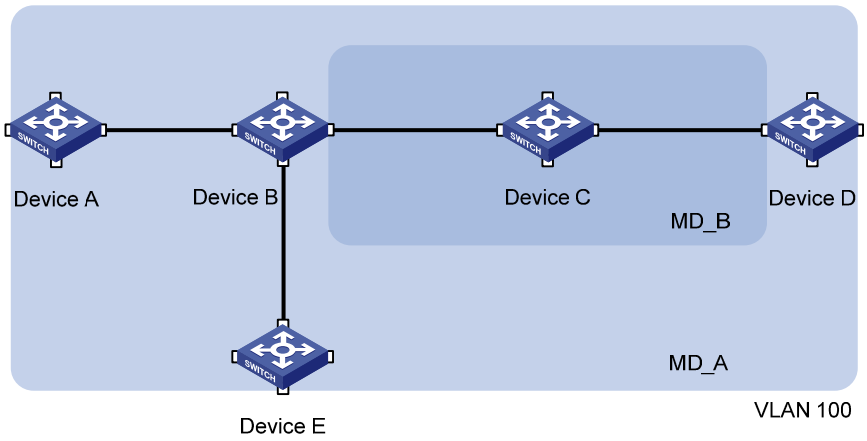
#### Maintenance domain

A maintenance domain (MD) defines the network where CFD plays its role. The MD boundary is defined by some maintenance association end points MEPs configured on the ports. A MD is identified by an MD name.

To locate faults exactly, CFD introduces eight levels (from 0 to 7) to MDs. The bigger the number, the higher the level and the larger the area covered. Domains can touch or nest (if the outer domain has a higher level than the nested one) but cannot intersect or overlap.

MD levels facilitate fault location and make fault location more accurate. As shown in Figure 1-1, MD_A in light blue nests MD_B in dark blue. If a connectivity fault is detected at the boundary of MD_A, any of the devices in MD_A, including Device A through Device E, may fail. In this case, if a connectivity fault is also detected at the boundary of MD_B, the failure points may be any of Device B through Device D. If the devices in MD_B operate normally, you can be sure that at least Device C is operational.

**Figure 1-1** Two nested MDs




CFD exchanges messages and performs operations on a per-domain basis. By planning MDs properly in a network, you can use CFD to locate failure points rapidly.

## Maintenance association

A maintenance association (MA) is a set of maintenance points (MPs) in a MD. An MA is identified by the “MD name + MA name”.

An MA serves a VLAN. Packets sent by the MPs in an MA carry the corresponding VLAN tag. An MP can receive packets sent by other MPs in the same MA.

## Maintenance point

An MP is configured on a port and belongs to an MA. MPs fall into two types: maintenance association end points (MEPs) and maintenance association intermediate points (MIPs).

- MEP

Each MEP is identified by an integer called a MEP ID. The MEPs of an MD define the range and boundary of the MD. The MA and MD that a MEP belongs to define the VLAN attribute and level of the packets sent by the MEP. MEPs fall into inward-facing MEPs and outward-facing MEPs.

The level of a MEP determines the levels of packets that the MEP can process. The packets transmitted from a MEP carry the level of the MEP. An MEP forwards packets at a higher level and processes packet of its level or lower. The processing procedure is specific to packets in the same VLAN. Packets of different VLANs are independent.

The direction of a MEP determines the position of the MD relative to the port. In Figure 1-2, outward-facing MEPs are configured on the two ports. In Figure 1-3, inward-facing MEPs are configured on the two ports.

An outward-facing MEP communicates through the wire side connected to the port; an inward-facing MEP communicates through the relay function side.

**Figure 1-2** Outward-facing MEP

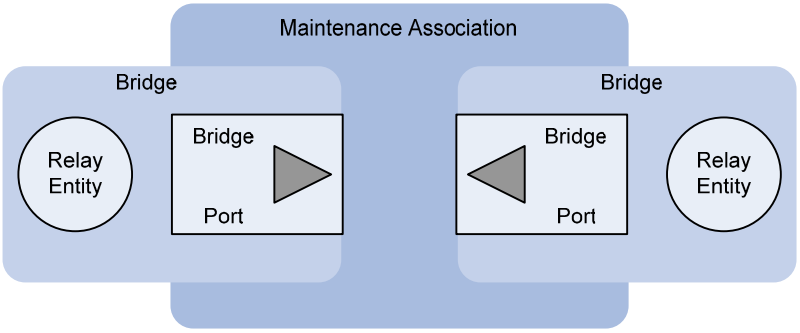
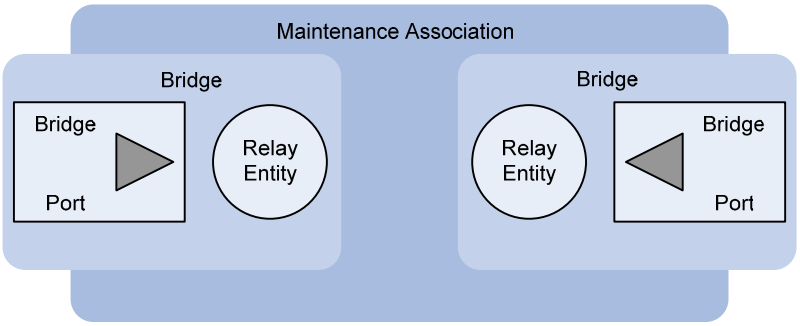



**Figure 1-3** Inward-facing MEP



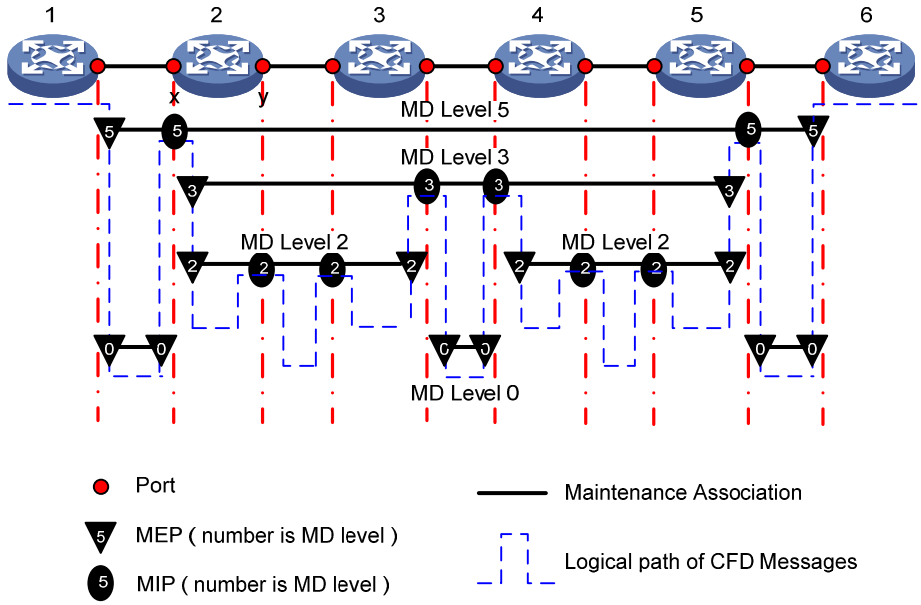

- MIP

A MIP is internal to an MD. It cannot send CFD packets actively; however, it can handle and respond to CFD packets. The MA and MD that a MIP belongs to define the VLAN attribute and level of the packets received.

By cooperating with MEPs, a MIP can perform a function similar to ping and traceroute. Like a MEP, a MIP forwards packets at a higher level without any processing.

Figure 1-4 demonstrates a grading example of the CFD module. In the figure, there are six devices, labeled 1 through 6 respectively. Suppose each device has two ports, and MEPs and MIPs are configured on some of these ports. Four levels of MDs are designed in this example, the bigger the number, the higher the level and the larger the area covered. In this example, the X port of device 2 is configured with the following MPs: a level 5 MIP, a level 3 inward-facing MEP, a level 2 inward-facing MEP, and a level 0 outward-facing MEP.

**Figure 1-4** Levels of MPs




## Basic Functions of CFD

CFD works effectively only in properly-configured networks. Its functions, which are implemented through the MPs, include:

- Continuity check (CC);
- Loopback (LB)
- Linktrace (LT)

### Continuity check

Continuity check is responsible for checking the connectivity between MEPs. Connectivity faults are usually caused by device faults or configuration errors. This function is implemented through periodic sending of continuity check messages (CCMs) by the MEPs. As a multicast message, a CCM sent by one MEP is intended to be received by all the other MEPs in the same MA. If a MEP fails to receive the CCMs within 3.5 sending periods, the link is regarded as faulty and a corresponding log is generated. When multiple MEPs send CCMs at the same time, the multipoint-to-multipoint link check is achieved.

### Loopback

Similar to ping at the IP layer, loopback is responsible for verifying the connectivity between a local device and a remote device. To implement this function, the local MEP sends loopback messages (LBMs) to the remote MEP. Depending on whether the local MEP can receive a loopback reply message (LBR) from the remote MEP, the link state between the two can be verified. LBMs and LBRs are unicast messages. They are used to verify the connectivity between two points.

### Linktrace

Linktrace is responsible for identifying the path between the source MEP and the destination MEP. This function is implemented in the following way: the source MEP multicasts linktrace messages (LTMs) to the destination MEP. After receiving the messages, the destination MEP and the MIPs that the LTMs pass send back linktrace reply messages (LTRs) to the source MEP. Based on the reply messages, the

source MEP can identify the path to the destination MEP. Note that LTMs are multicast frames while LTRs are unicast frames.

### Protocols and Standards

The CFD function is implemented in accordance with IEEE P802.1ag.

## CFD Configuration Task List

For CFD to work effectively, you should first design the network by performing the following tasks:

- Grade the MDs in the entire network, and define the boundary of each MD.
- Assign a name for each MD. Make sure that the same MD has the same name on different devices.
- Define the MA in each MD according to the VLAN you want to monitor.
- Assign a name for each MA. Make sure that the same MA in the same MD has the same name on different devices.
- At the edges of MD and MA, MPs should be designed at the device port. MEPs can be designed on devices or ports that are not at the edges.

Complete the following tasks to configure CFD:

| Tasks | Remarks |
|---|---|
| Basic Configuration Tasks | Required<br>These configurations are the foundation for other configuration tasks. |
| Configuring CC on MEPs | Required<br>Configuring the MEPs to send CCMs to manage link connectivity |
| Configuring LB on MEPs | Optional<br>Checking link state by testing link connectivity |
| Configuring LT on MEPs | Optional<br>Tracing link fault and finding the path between the source MEP and target MEP |

**Note**

- A port blocked by STP cannot receive, send, or respond to CFD messages, however, if the port is configured as an outward-facing MEP, it can still receive and send CCM messages even if it is blocked by STP.
- Only Ethernet ports support CFD.

## Basic Configuration Tasks

Basic configuration tasks include:

- Configuring Service Instance
- Configuring MEP
- Configuring MIP Generation Rules

**Note**

Based on the network design, you should configure MEPs or the rules for generating MIPs on each device. However, before doing this you must first configure the service instance.

## Configuring Service Instance

A service instance is indicated by an integer to represent an MA in an MD. The MD and MA define the level and VLAN attribute of the messages handled by the MPs in a service instance.

Follow these steps to configure a service instance:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable CFD | **cfd enable** | Required<br>CFD is disabled by default. |
| Create an MD | **cfd md** *md-name* **level** *level-value* | Required<br>Not created by default |
| Create an MA | **cfd ma** *ma-name* **md** *md-name* **vlan** *vlan-id* | Required<br>Not created by default |
| Create a service instance | **cfd service-instance** *instance-id* **md** *md-name* **ma** *ma-name* | Required<br>Not created by default |

**Caution**

- These configuration tasks are the foundation for other CFD configuration tasks.
- The last three steps in the table above must be performed strictly in order.

## Configuring MEP

MEPs are functional entities in a service instance. CFD is implemented through operations on MEPs, which provides such functions as CC, LB, LT and gives prompts on error CCMs and cross connections. As a MEP is configured on a service instance, the MD level and VLAN attribute of the service instance become the attribute of the MEP.

Follow these steps to configure a MEP:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure a MEP | **cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** \| **outbound** } | Required<br>Not configured by default |

| To do... | Use the command... | Remarks |
|---|---|---|
| Configure a remote MEP for a MEP in the same service instance | **cfd remote-mep** *remote-mep-id* **service-instance** *instance-id* **mep** *mep-id* | Required<br>No remote MEP is configured for a MEP by default. |
| Enable the MEP | **cfd mep service-instance** *instance-id* **mep** *mep-id* **enable** | Required<br>Disabled by default |

## Configuring MIP Generation Rules

As functional entities in a service instance, MIPs deal with LBM and LTM messages.

MIPs are generated on each port according to some rules. You can choose appropriate MIP generation rules based on your network design.

Follow these steps to configure the rules for generating MIPs:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the rules for generating MIPs | **cfd mip-rule** { **explicit** \| **default** } **service-instance** *instance-id* | Required<br>By default, neither the MIPs nor the rules for generating MIPs are configured. |

MIPs are generated on each port automatically according to the rules specified in the **cfd mip-rule** command. If a port has no MIP, the system will check the MAs in each MD (from low to high levels), and follow the rules in Table 1-1 to create or not create MIPs (within a single VLAN):

**Table 1-1** Rules for generating MIP

| MIP exists on low level MA | The cfd mip-rule command is configured as | MEP exists on low level MA | Create MIP or not |
|---|---|---|---|
| Yes | — | — | No |
| No | Explicit | No | No |
| | | Yes | Yes |
| | Default | — | Yes |

Each of the following actions or cases can cause MIPs to be created or deleted after you have configured the **cfd mip-rule** command:

- Enabling CFD (use the **cfd enable** command)
- Creating or deleting the MEPs on a port
- Changes occur to the VLAN attribute of a port
- The rule specified in the **cfd mip-rule** command changes

# Configuring CC on MEPs

After the CC function is configured, MEPs can send CCMs mutually to check the connectivity between them.

## Configuration Prerequisites

Before configuring this function, you should first complete the MEP configuration.

## Configuring Procedure

Follow these steps to configure CC on a MEP:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the interval field value in the CCM messages sent by MEPs | **cfd cc interval** *interval-field-value* **service-instance** *instance-id* | Optional<br>By default, the interval filed value is 4. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable CCM sending on a MEP | **cfd cc service-instance** *instance-id* **mep** *mep-id* **enable** | Required<br>Disabled by default |

The relationship between the interval field value in the CCM messages, the interval between CCM messages and the timeout time of the remote MEP is illustrated in Table 1-2.

**Table 1-2** Relationship of the interval field value, the interval between CCM messages and the timeout time of the remote MEP

| The interval field value | The interval between CCM messages | The timeout time of the remote MEP |
|---|---|---|
| 4 | 1 second | 3.5 seconds |
| 5 | 10 second | 35 seconds |
| 6 | 60 seconds | 210 seconds |
| 7 | 600 seconds | 2100 seconds |

**Caution**

On different devices, the MEPs belonging to the same MD and MA should be configured with the same time interval for CCMs sending.

# Configuring LB on MEPs

The LB function can verify the link state between two ends after CC detects a link fault.

## Configuration Prerequisites

Before configuring this function, you should first complete the MEP and MIP configuration tasks.

### Configuration Procedure

Follow these steps to configure LB on MEP:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable LB | **cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* \| **target-mac** *mac-address* } [ **number** *loopback-number* ] | Required<br>Disabled by default |

## Configuring LT on MEPs

LT can trace the path between the specified MEP and the target MEP, and can also locate link faults by sending LT messages automatically. The two functions are implemented in the following way:

- To implement the first function, the specified MEP first sends LTM messages to the target MEP. Based on the LTR messages in response to the LTM messages, the path between the two MEPs can be identified.
- In the latter case, after LT messages automatic sending is enabled, if a MEP fails to receive the CCMs from the remote MEP within 3.5 sending intervals, the link between the two is regarded as faulty and LTMs will be sent out. Based on the LTRs that echo back, the fault source can be located.

### Configuration Prerequisites

Before configuring this function, you should first complete MEP and MIP configuration tasks.

### Finding the Path Between a Source MEP and a Target MEP

Follow these steps to find the path between a source MEP and a target MEP:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Find the path between a source MEP and a target MEP | **cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* \| **target-mac** *mac-address* } [ **ttl** *ttl-value* ] [ **hw-only** ] | Required |

### Enabling Automatic LT Messages Sending

Follow these steps to enable automatic LT messages sending:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable automatic LT messages sending | **cfd linktrace auto-detection** [ **size** *size-value* ] | Required<br>Disabled by default |

# Displaying and Maintaining CFD

| To do... | Use the command... | Remarks |
|---|---|---|
| Display CFD status | **display cfd status** | Available in any view |
| Display MD configuration information | **display cfd md** | Available in any view |
| Display MA configuration information | **display cfd ma** [ [ *ma-name* ] **md** *md-name* ] | Available in any view |
| Display service instance configuration information | **display cfd service-instance** [ *instance-id* ] | Available in any view |
| Display MP information | **display cfd mp** [ **interface** *interface-type interface-number* ] | Available in any view |
| Display the attribute and running information of the MEPs | **display cfd mep** *mep-id* **service-instance** *instance-id* | Available in any view |
| Display LTR information received by a MEP | **display cfd linktrace-reply** [ **service-instance** *instance-id* [ **mep** *mep-id* ] ] | Available in any view |
| Display the information of a remote MEP | **display cfd remote-mep service-instance** *instance-id* **mep** *mep-id* | Available in any view |
| Display the content of the LTR that responds to LTM messages | **display cfd linktrace-reply auto-detection** [ **size** *size-value* ] | Available in any view |

# CFD Configuration Examples

## Configuring Service Instance

### Network requirements

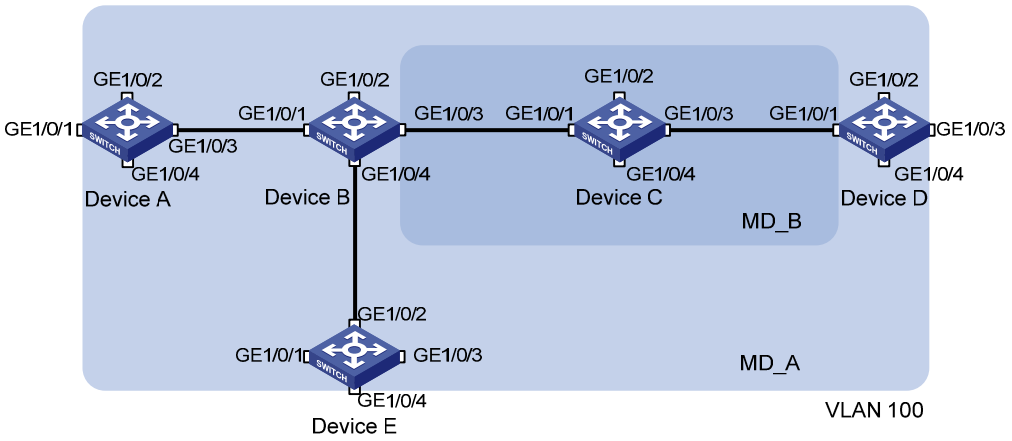
As shown in Figure 1-5, there are five devices in the MDs. Each device has four ports belonging to VLAN 100. The light blue square frame and the blue one specify two different MDs.

- Two MDs, MD_A (indicated by the light blue square frame, with level 5) and MD_B (indicated by the blue square frame, with level 3)) are designed in this network.
- Define the edge ports of each MD, and define the MD of each port.
- The VLAN IDs of each MA in the two MDs are all 100.

According to the network diagram as shown in Figure 1-5, You should perform the following configurations:

- Configure MD_A on Device A and Device E
- Configure MD_B on Device C
- Configure MD_A and MD_B on Device B and Device D
- Configure an MA in each MD
- Configure a service instance for each MA

**Figure 1-5** Network diagram for MD configuration




### Configuration procedure

1) Configuration on Device A (configuration on Device E is the same as that on Device A)

```
<DeviceA> system-view
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
[DeviceA] cfd ma MA_MD_A md MD_A vlan 100
[DeviceA] cfd service-instance 1 md MD_A ma MA_MD_A
```

2) Configuration on Device C

```
<DeviceC> system-view
[DeviceC] cfd enable
[DeviceC] cfd md MD_B level 3
[DeviceC] cfd ma MA_MD_B md MD_B vlan 100
[DeviceC] cfd service-instance 2 md MD_B ma MA_MD_B
```

3) Configuration on Device B (configuration on Device D is the same as that on Device B)

```
<DeviceB> system-view
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd ma MA_MD_A md MD_A vlan 100
[DeviceB] cfd service-instance 1 md MD_A ma MA_MD_A
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd ma MA_MD_B md MD_B vlan 100
[DeviceB] cfd service-instance 2 md MD_B ma MA_MD_B
```

After the above configuration, you can use the commands **display cfd md**, **display cfd ma** and **display cfd service-instance** to verify your configuration.

## Configuring MEP and Enabling CC on it

### Network requirements

After finishing service instance configuration, you can start to design the MEPs.

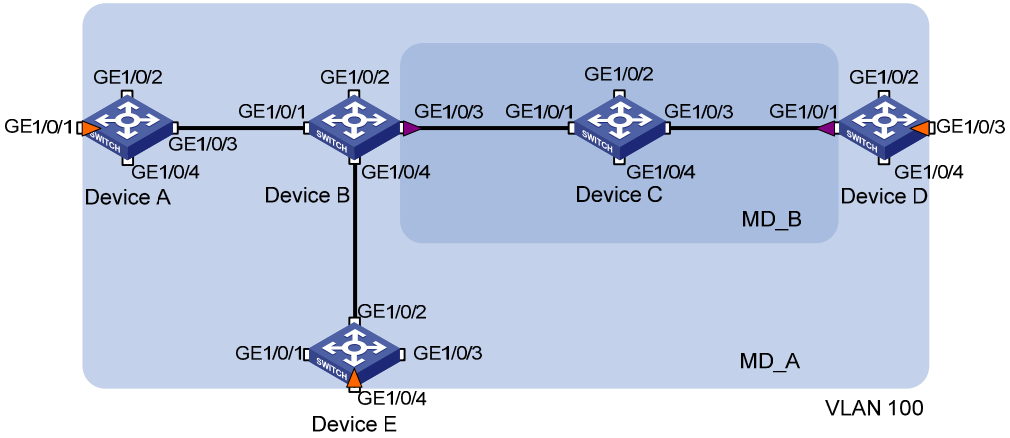
- MEPs are configured at the edge or border of MDs. Find the edge port of each MD.
- Decide the MEP direction (inward-facing or outward-facing) on each edge port based on the MD position.
- Assign a unique ID to each MEP in an MA.

- Decide the remote MEP for each MEP, and enable these MEPs.

According to the network diagram as shown in Figure 1-6, perform the following configurations:

- In MD_A, there are three edge ports: GigabitEthernet 1/0/1 on Device A, GigabitEthernet 1/0/3 on Device D and GigabitEthernet 1/0/4 on Device E. Configure inward-facing MEPs on these ports respectively.
- In MD_B, there are two edge ports: GigabitEthernet 1/0/3 on Device B and GigabitEthernet 1/0/1 on Device D. Configure outward-facing MEPs on the two ports respectively.
- In MD_A and MD_B, each MEP checks the messages from other MEPs.

**Figure 1-6** Network diagram of MD and MEP configuration




## Configuration procedure

1) On Device A

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] cfd remote-mep 5001 service-instance 1 mep 1001
[DeviceA-GigabitEthernet1/0/1] cfd remote-mep 4002 service-instance 1 mep 1001
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
```

2) On Device B

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd mep 2001 service-instance 2 outbound
[DeviceB-GigabitEthernet1/0/3] cfd remote-mep 4001 service-instance 2 mep 2001
[DeviceB-GigabitEthernet1/0/3] cfd mep service-instance 2 mep 2001 enable
[DeviceB-GigabitEthernet1/0/3] cfd cc service-instance 2 mep 2001 enable
```

3) On Device D

```
<DeviceD> system-view
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/1] cfd remote-mep 2001 service-instance 2 mep 4001
[DeviceD-GigabitEthernet1/0/1] cfd mep service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound
```

```
[DeviceD-GigabitEthernet1/0/3] cfd remote-mep 1001 service-instance 1 mep 4002
[DeviceD-GigabitEthernet1/0/3] cfd remote-mep 5001 service-instance 1 mep 4002
[DeviceD-GigabitEthernet1/0/3] cfd mep service-instance 1 mep 4002 enable
[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 1 mep 4002 enable
```

4) On Device E

```
<DeviceE> system-view
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd mep 5001 service-instance 1 inbound
[DeviceE-GigabitEthernet1/0/4] cfd remote-mep 1001 service-instance 1 mep 5001
[DeviceE-GigabitEthernet1/0/4] cfd remote-mep 4002 service-instance 1 mep 5001
[DeviceE-GigabitEthernet1/0/4] cfd mep service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet1/0/4] cfd cc service-instance 1 mep 5001 enable
```

After the above configuration, you can use the commands **display cfd mp** and **display cfd mep** to verify your configuration.

## Configuring the Rules for Generating MIPs

### Network requirements

After finishing MEP configuration, you can continue to configure the MIPs.

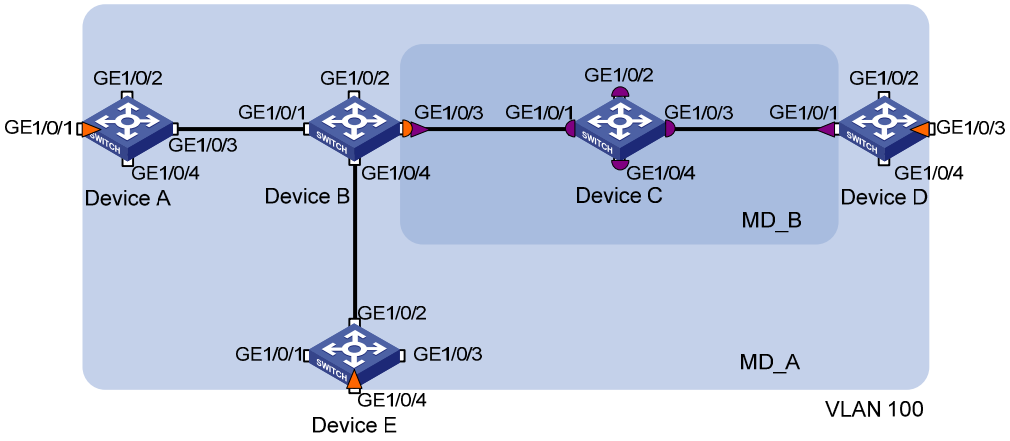
MIPs, which are generated by some rules, are configured in the following way:

- Decide the device on which MIPs are to be configured.
- Choose suitable rules for MIP generation. By default, MIP is not configured on a device. If MIPs are to be configured on each port in the MD, you should choose the **default** rule. If MIPs are to be configured only when the low level MDs having MEP, you should choose the **explicit** rule.

According to the diagram as shown in Figure 1-7, perform the following configurations:

- In MD_A, Device B is designed to have MIPs when its port is configured with low level MEPs. In this case, port GigabitEthernet 1/0/3 is configured with MEPs of MD_B, and the MIPs of MD_A can be configured on this port. Based on the design, you should configure the MIP generation rule of MD_A to explicit on Device B.
- The MIPs of MD_B are designed on Device C, and are configured on all ports. Based on this design, the MIP generation rule should be configured as default.

**Figure 1-7** Network diagram of MD and MP configuration



### Configuration procedure

1) Configure Device B

```
<DeviceB> system-view
[DeviceB] cfd mip-rule explicit service-instance 1
```

2) Configure Device C

```
<DeviceC> system-view
[DeviceC] cfd mip-rule default service-instance 2
```

After the above operation, you can use the **display cfd mp** command to verify your configuration.

## Configuring LB on MEPs

### Network requirements

Use the LB function to trace the fault source after CC detects a link fault.

As shown in Figure 1-6, enable LB on Device A so that Device A can send LBM messages to MEPs on Device D.

### Configuration procedure

# Configure Device A

```
<DeviceA> system-view
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 4002
```

## Configuring LT on MEPs

### Network requirements

Use the LT function to find the path and locate the fault after you obtain the state of the entire network through the CC.

As shown in Figure 1-6, enable LT on Device A so that Device A can send LTM messages to the MEP on Device D.

### Configuration procedure

# Configure Device A

```
<DeviceA> system-view
[DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 4002
```

# Table of Contents

# 1 RRPP Configuration

When configuring RRPP, go to these sections for information you are interested in:



## RRPP Overview

The Rapid Ring Protection Protocol (RRPP) is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes in the event that a link is disconnected on the ring.

Compared with the IEEE spanning tree protocols, RRPP features the following:

- Fast topology convergence
- Convergence time independent of Ethernet ring size

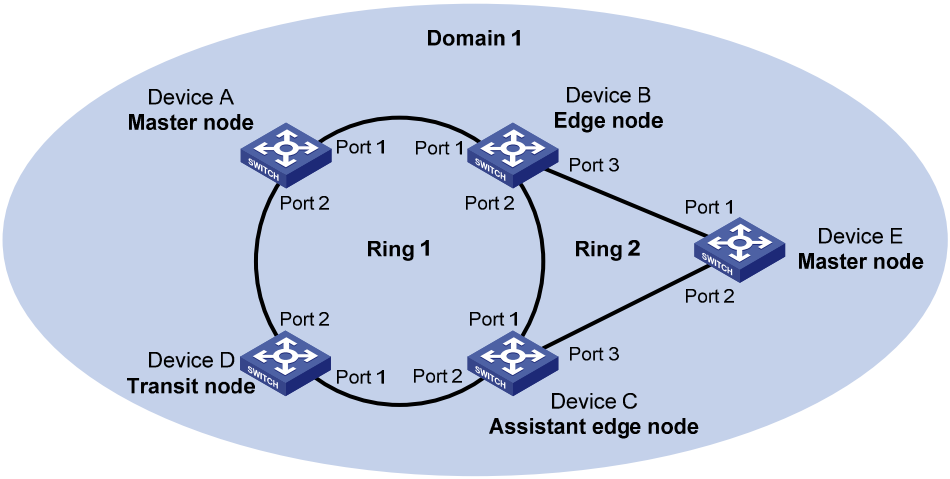
### Background

Metropolitan area networks (MANs) and enterprise networks usually use the ring structure to improve reliability. However, services will be interrupted if any node in the ring network fails. A ring network usually uses Resilient Packet Ring (RPR) or Ethernet rings. RPR is high in cost as it needs dedicated hardware. Contrarily, the Ethernet ring technology is more mature and economical, so it is more and more widely used in MANs and enterprise networks.

Currently, both Spanning Tree Protocol (STP) and RRPP can be used to eliminate Layer-2 loops. STP is mature; however, it takes several seconds to converge. RRPP is an Ethernet ring-specific data link layer protocol, and converges faster than STP. Additionally, the convergence time of RRPP is independent of the number of nodes in the Ethernet ring, and therefore, RRPP can be applied to large-diameter networks.

## Basic Concepts in RRPP

**Figure 1-1** RRPP networking diagram




### RRPP domain

The interconnected devices with the same domain ID and control VLANs constitute an RRPP domain. An RRPP domain contains the following elements: primary ring, subring, control VLAN, master node, transit node, primary port, secondary port, common port, and edge port.

As shown in Figure 1-1, Domain 1 is an RRPP domain, including two RRPP rings: Ring 1 and Ring 2. All the nodes on the two RRPP rings belong to the RRPP domain.

### RRPP ring

A ring-shaped Ethernet topology is called an RRPP ring. RRPP rings fall into two types: primary ring and subring. You can configure a ring as either the primary ring or a subring by specifying its ring level. The primary ring is of level 0, while a subring is of level 1. An RRPP domain contains multiple RRPP rings, one serving as the primary ring and the others serving as subrings.

As shown in Figure 1-1, Domain 1 contains two RRPP rings: Ring 1 and Ring 2. The level of Ring 1 is set to 0, that is, Ring 1 is configured as the primary ring; the level of Ring 2 is set to 1, that is, Ring 2 is configured as a subring.

A ring can be in one of the following two states:

- Health state: All the physical links on the Ethernet ring are connected.
- Disconnect state: Some physical links on the Ethernet ring are broken.

### Control VLAN and data VLAN

In an RRPP domain, a control VLAN is a VLAN dedicated to transferring RRPP packets.

On a device, the ports accessing an RRPP ring belong to the control VLANs of the ring, and only such ports can join the control VLANs.

An RRPP domain is configured with two control VLANs: one primary control VLAN, which is the control VLAN for the primary ring; one secondary control VLAN, which is the control VLAN for subrings. All subrings in the same RRPP domain share the same secondary control VLAN. After you specify a VLAN as the primary control VLAN, the system automatically configures the VLAN whose ID is the primary control VLAN ID plus one as the secondary control VLAN.

IP address configuration is prohibited on the control VLAN interfaces.

A data VLAN is a VLAN dedicated to transferring data packets. Both RRPP ports and non-RRPP ports can be assigned to a data VLAN.

### Node

Each device on an RRPP ring is referred to as a node. The role of a node is configurable. There are the following node roles:

- Master node: Each ring has one and only one master node. The master node initiates the polling mechanism and determines the operations to be performed after a change in topology.
- Transit node: Transit nodes include all the nodes except the master node on the primary ring and all the nodes on subrings except the master nodes and the nodes where the primary ring intersects with the subrings. A transit node monitors the state of its directly-connected RRPP links and notifies the master node of the link state changes, if any. Based on the link state changes, the master node decides the operations to be performed.
- Edge node: A node residing on both the primary ring and a subring at the same time. An edge node is a special transit node that serves as a transit node on the primary ring and an edge node on the subring.
- Assistant-edge node: A node residing on both the primary ring and a subring at the same time. An assistant-edge node is a special transit node that serves as a transit node on the primary ring and an assistant-edge node on the subring. This node works in conjunction with the edge node to detect the integrity of the primary ring and perform loop guard.

As shown in Figure 1-1, Ring 1 is the primary ring and Ring 2 is a subring. Device A is the master node of Ring 1, Device B, Device C and Device D are the transit nodes of Ring 1. Device E is the master node of Ring 2, Device B is the edge node of Ring 2, and Device C is the assistant-edge node of Ring 2.

### Primary port and secondary port

Each master node or transit node has two ports connected to an RRPP ring, one serving as the primary port and the other serving as the secondary port. You can determine the role of a port.

1) In terms of functionality, the difference between the primary port and the secondary port of a master node is:

- The primary port and the secondary port are designed to play the role of sending and receiving loop-detect packets respectively.
- When an RRPP ring is in Health state, the secondary port of the master node will logically deny data VLANs and permit only the packets of the control VLANs.
- When an RRPP ring is in Disconnect state, the secondary port of the master node will permit data VLANs, that is, forward packets of data VLANs.

2) In terms of functionality, there is no difference between the primary port and the secondary port of a transit node. Both are designed for transferring protocol packets and data packets over an RRPP ring.

As shown in Figure 1-1, Device A is the master node of Ring 1. Port 1 and Port 2 are the primary port and the secondary port of the master node on Ring 1 respectively. Device B, Device C, and Device D are the transit nodes of Ring 1. Their Port 1 and Port 2 are the primary port and the secondary port on Ring 1 respectively.

### Common port and edge port

The ports connecting the edge node and assistant-edge node to the primary ring are common ports. The ports connecting the edge node and assistant-edge node only to the subrings are edge ports.

As shown in Figure 1-1, Device B and Device C lie on Ring 1 and Ring 2. Device B's Port 1 and Port 2 and Device C's Port 1 and Port 2 access the primary ring, so they are common ports. Device B's Port 3 and Device C's Port 3 access only the subring, so they are edge ports.

### RRPP ring group

To reduce Edge-Hello traffic, you can configure a group of subrings on the edge node or assistant-edge node. For information about Edge-Hello packets, refer to RRPP Packets. You must configure a device as the edge node of these subrings, and another device as the assistant-edge node of these subrings. Additionally, the subrings of the edge node and assistant-edge node must connect to the same subring packet tunnels in major ring (SRPTs), so that Edge-Hello packets of the edge node of these subrings travel to the assistant-edge node of these subrings over the same link.

A ring group configured on the edge node is called an edge node ring group, and a ring group configured on an assistant-edge node is called an assistant-edge node ring group. Up to one subring in an edge node ring group is allowed to send Edge-Hello packets.

## RRPP Packets

Table 1-1 shows the types of RRPP packets and their functions.

**Table 1-1** RRPP packet types and their functions

| Type | Description |
|---|---|
| Hello | The master node initiates Hello packets to detect the integrity of a ring in a network. |
| Link-Down | The transit node, the edge node or the assistant-edge node initiates Link-Down packets to notify the master node of the disappearance of a ring in case of a link failure. |
| Common-Flush-FDB | The master node initiates Common-Flush-FDB packets to instruct the transit nodes to update their own MAC entries and ARP/ND entries when an RRPP ring transits to Disconnect state. |
| Complete-Flush-FDB | The master node initiates Complete-Flush-FDB packets to instruct the transit nodes to update their own MAC entries and ARP/ND entries, and release blocked ports from being blocked temporarily when an RRPP ring transits to Health state. |
| Edge-Hello | The edge node initiates Edge-Hello packets to examine the links of the primary ring between the edge node and the assistant-edge node. |
| Major-Fault | The assistant-edge node initiates Major-Fault packets to notify the edge node of a failure when a link of primary ring between edge node and assistant-edge node is torn down. |

## Hello and Fail Timers

When RRPP checks the link state of an Ethernet ring, the master node sends Hello packets out the primary port according to the Hello timer and determines whether its secondary port receives the Hello packets based on the Fail timer.

- The Hello timer specifies the interval at which the master node sends Hello packets out the primary port.
- The Fail timer specifies the maximum delay between the master node sending Hello packets out the primary port and the secondary port receiving the Hello packets from the primary port. If the

secondary port receives the Hello packets sent by the local master node before the Fail timer expires, the overall ring is in Health state. Otherwise, the ring transits into Disconnect state.

---

**Note**

- In an RRPP domain, a transit node learns the Hello timer value and the Fail timer value on the master node through the received Hello packets, ensuring that all nodes in the ring network are consistent in the two timer settings.
- The Fail timer value must be greater than or equal to three times of the Hello timer value.
- In a dual-homed-ring network, to avoid temporary loops when the primary ring fails, ensure that the difference between the Fail timer value on the master node of the subring and that on the master node of the primary ring is greater than twice the Hello timer value of the master node of the subring.

---

## How RRPP Works

### Polling mechanism

The polling mechanism is used by the master node of an RRPP ring to check the Health state of the ring network.

The master node sends Hello packets out its primary port periodically, and these Hello packets travel through each transit node on the ring in turn.

- If the ring is complete, the secondary port of the master node will receive Hello packets before the Fail timer expires and the master node will keep the secondary port blocked.
- If the ring is torn down, the secondary port of the master node will fail to receive Hello packets before the Fail timer expires. The master node will release the secondary port from blocking data VLANs while sending Common-Flush-FDB packets to instruct all transit nodes to update their own MAC entries and ARP/ND entries.

### Link down alarm mechanism

The transit node, the edge node or the assistant-edge node sends Link-Down packets to the master node immediately when they find any of its own ports belonging to an RRPP domain is down. Upon the receipt of a Link-Down packet, the master node releases the secondary port from blocking data VLANs while sending Common-Flush-FDB packet to instruct all the transit nodes, the edge nodes and the assistant-edge nodes to update their own MAC entries and ARP/ND entries. After each node updates its own entries, traffic is switched to the normal link.

### Ring recovery

The master node may find the ring is restored after a period of time after the ports belonging to the RRPP domain on the transit nodes, the edge nodes, or the assistant-edge nodes are brought up again. A temporary loop may arise in the data VLAN during this period. As a result, broadcast storm occurs.

To prevent temporary loops, non-master nodes block them immediately (and permit only the packets of the control VLAN to pass through) when they find their ports accessing the ring are brought up again. The blocked ports are activated only when the nodes are sure that no loop will be brought forth by these ports.

### Broadcast storm suppression mechanism in a multi-homed subring in case of SRPT failure

As shown in Figure 1-5, Ring 1 is the primary ring, and Ring 2 and Ring 3 are subrings. When the two SRPTs between the edge node and the assistant-edge node are down, the master nodes of Ring 2 and Ring 3 will open their respective secondary ports, and thus a loop among Device B, Device C, Device E, and Device F is generated. As a result, broadcast storm occurs.

In this case, to prevent generating this loop, the edge node will block the edge port temporarily. The blocked edge port is activated only when the edge node is sure that no loop will be brought forth when the edge port is activated.

### Load balancing

In a ring network, maybe traffic of multiple VLANs is transmitted at the same time. RRPP can implement load balancing for the traffic by transmitting traffic of different VLANs along different paths.

By configuring an individual RRPP domain for transmitting the traffic of the specified VLANs (referred to as protected VLANs) in a ring network, traffic of different VLANs can be transmitted according to different topologies in the ring network. In this way, load balancing is achieved.

As shown in Figure 1-6, Ring 1 is configured as the primary ring of Domain 1 and Domain 2, which are configured with different protected VLANs. Device A is the master node of Ring 1 in Domain 1; Device B is the master node of Ring 1 in Domain 2. With such configurations, traffic of different VLANs can be transmitted on different links, and thus, load balancing is achieved in a single-ring network.

### RRPP ring group

In an edge node ring group, only an activated subring with the lowest domain ID and ring ID can send Edge-Hello packets. In an assistant-edge node ring group, any activated subring that has received Edge-Hello packets will forward these packets to the other activated subrings. With an edge node ring group and an assistant-edge node group configured, only one subring sends and receives Edge-Hello packets, thus reducing CPU workload.

As shown in Figure 1-5, Device B is the edge node of Ring 2 and Ring 3, and Device C is the assistant-edge node of Ring 2 and Ring 3. Device B and Device C need to send or receive Edge-Hello packets frequently. If more subrings are configured or load balancing is configured for more multiple domains, Device B and Device C will send or receive a mass of Edge-Hello packets.

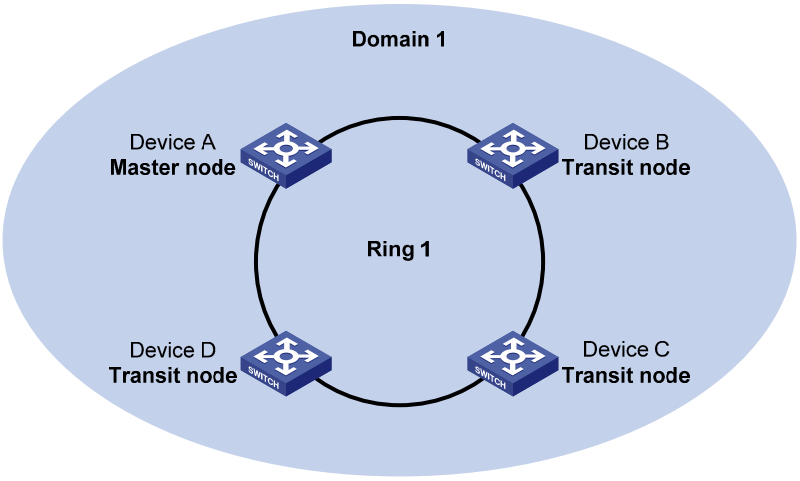
To reduce Edge-Hello traffic, you can assign Ring 2 and Ring 3 to a ring group configured on the edge node Device B, and assign Ring 2 and Ring 3 to a ring group configured on Device C. After such configurations, if all rings are activated, only Ring 2 on Device B sends Edge-Hello packets.

## Typical RRPP Networking

Here are several typical networking applications.

## Single ring

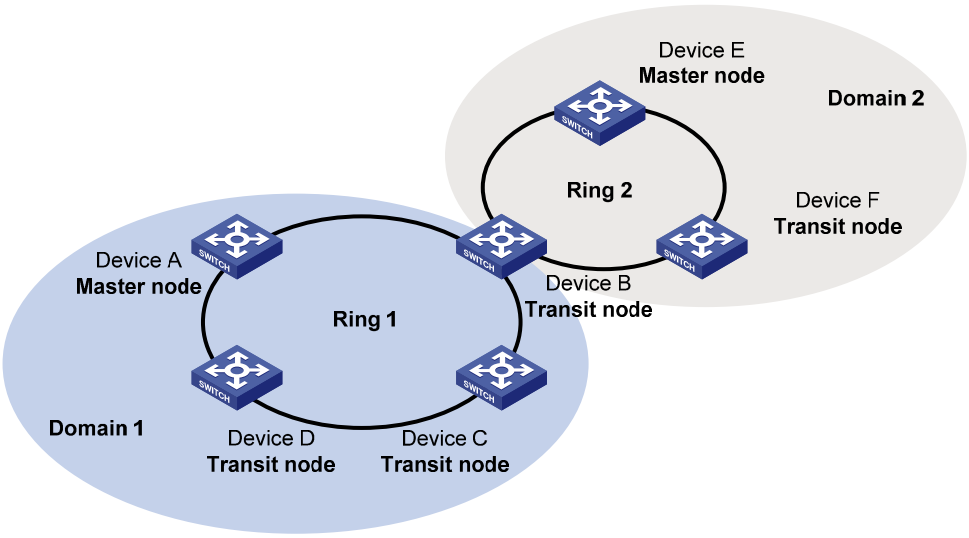
**Figure 1-2** Single ring




There is only a single ring in the network topology. In this case, you only need to define an RRPP domain.

## Tangent rings

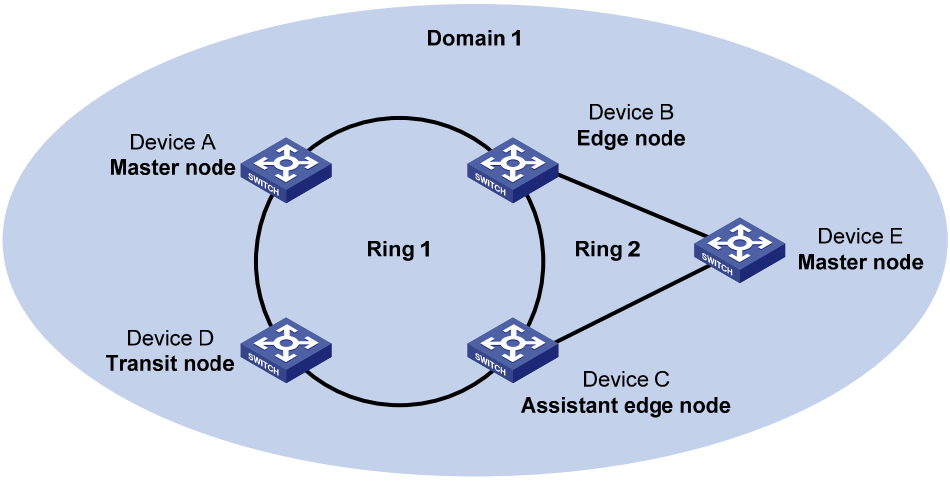
**Figure 1-3** Tangent rings




There are two or more rings in the network topology and only one common node between rings. In this case, you need to define an RRPP domain for each ring.

## Intersecting rings

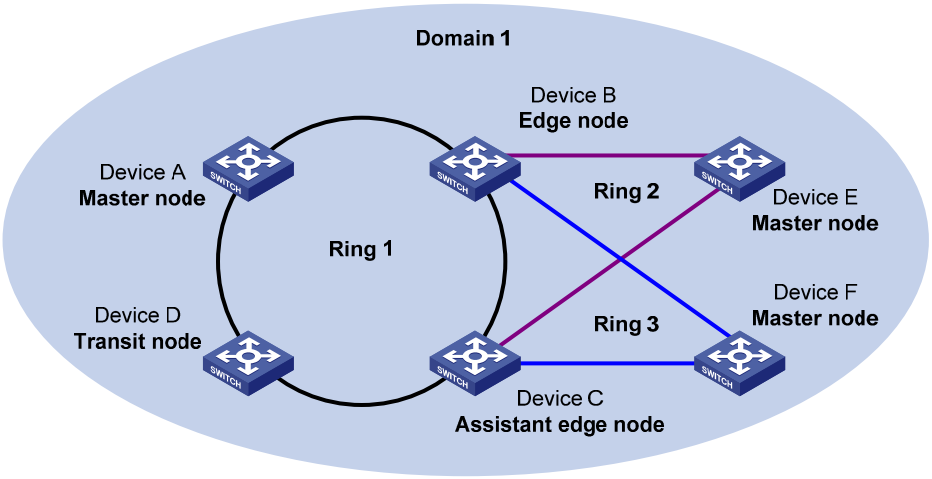
**Figure 1-4** Intersecting rings




There are two or more rings in the network topology and two common nodes between rings. In this case, you only need to define an RRPP domain, and set one ring as the primary ring and the other rings as subrings.

## Dual homed rings

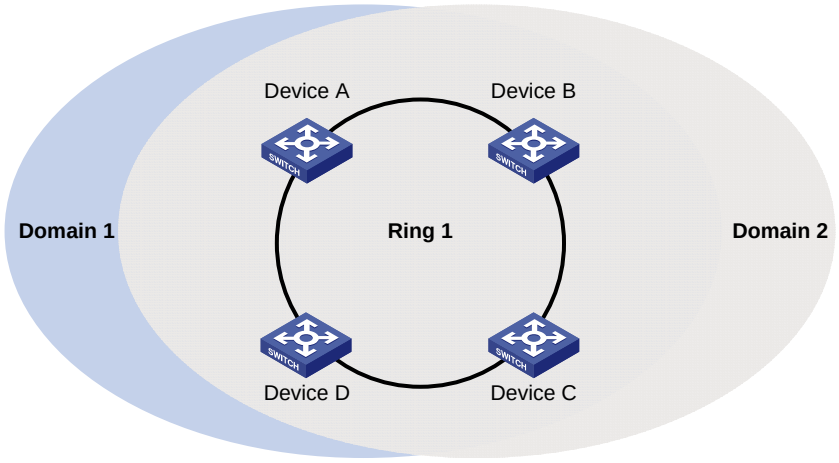
**Figure 1-5** Dual homed rings




There are two or more rings in the network topology and two similar common nodes between rings. In this case, you only need to define an RRPP domain, and set one ring as the primary ring and the other rings as subrings.

## Single-ring load balancing

**Figure 1-6** Network diagram for single-ring load balancing

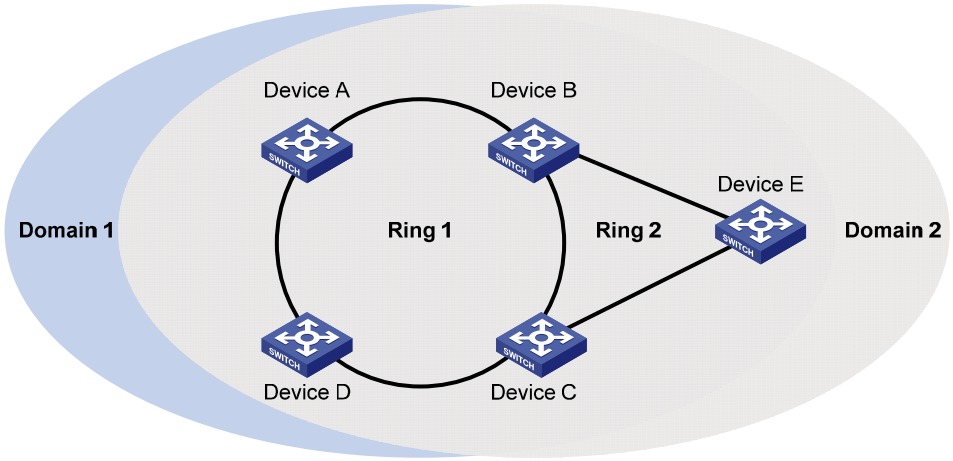



In a single-ring network, you can achieve load balancing by configuring multiple domains.

As shown in Figure 1-6, Ring 1 is configured as the primary ring of both Domain 1 and Domain 2. In Domain 1, Device A is configured as the master node of Ring 1; in Domain 2, Device B is configured as the master node of Ring 1. Such configurations enable the ring to block different links based on VLANs, thus achieving single-ring load balancing.

## Intersecting-ring load balancing

**Figure 1-7** Network diagram for intersecting-ring load balancing




In an intersecting-ring network, you can also achieve load balancing by configuring multiple domains.

As shown in Figure 1-7, Ring 1 is the primary ring and Ring 2 is the subring in both Domain 1 and Domain 2. Domain 1 and Domain 2 are configured with different protected VLANs. Device A is configured as the master node of Ring 1 in Domain 1; Device D is configured as the master node of Ring 1 in Domain 2. Device E is configured as the master node of Ring 2 in both Domain 1 and Domain 2. However, different ports on Device E are blocked in Domain 1 and Domain 2. After such configurations, you can enable traffic of different VLANs to travel over different paths in the subring and primary ring, thus achieving intersecting-ring load balancing.

### Protocols and Standards

RFC 3619 *Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1* is related to RRPP.

## RRPP Configuration Task List

**Caution**

- RRPP does not have an auto election mechanism, so you must configure each node in the ring network properly for RRPP to monitor and protect the ring network.
- Before configuring RRPP, you need to construct a ring-shaped Ethernet topology physically.

You can create RRPP domains based on service planning, specify control VLANs and data VLANs for each RRPP domain, and then determine the ring roles and node roles based on the traffic paths in each RRPP domain. You can configure devices through the following configurations.

Complete the following tasks to configure RRPP:

| Task | Description |
|---|---|
| Configuring Master Node | Required |
| Configuring Transit Node | Optional |
| Configuring Edge Node | Optional |
| Configuring Assistant Edge Node | Optional |
| Configuring Ring Group | Optional<br>To reduce Edge-Hello traffic, you can adopt the ring group mechanism, that is, assign subrings with the same edge node/assistant-edge node to a ring group. |

**Caution**

- It is recommended to configure the primary ring first and then the subring when you configure an RRPP domain. Moreover, a Ring ID cannot be applied to more than one RRPP ring in one RRPP domain.
- If a device lies on multiple RRPP rings in an RRPP domain, only one primary ring exists. The device serves as either an edge node or an assistant-edge node on the subrings.
- The total number of rings configured on a device in all RRPP domains cannot be greater than 16.
- Modification of node mode, port role and ring level of an RRPP ring is prohibited after configuration. If needed, you must first delete the existing configuration.
- During load balancing configuration, different protected VLANs must be configured for different domains.

Ports connected to an RRPP ring must meet the following conditions:

- The link type of these ports must be trunk.
- They must be Layer 2 GE ports.
- They must not be member ports of any aggregation group or smart link group.
- STP is disabled on them.
- The 802.1p priority of trusted packets on the ports is configured, so that RRPP packets take higher precedence than data packets when passing through the ports.
- Do not enable OAM remote loopback function on an RRPP port. Otherwise, this may cause temporary broadcast storm.
- You are recommended not to configure physical-link-state change suppression time on a port accessing an RRPP ring to accelerate topology convergence. For details, refer to *Ethernet Interface Configuration* in the *Access Volume*.

---

**Note**

- If you need to transparently transmit RRPP packets on a device without enabling RRPP, you must ensure only the two ports accessing an RRPP ring permit the packets of the control VLAN. Otherwise, the packets from other VLANs may go into the control VLAN in transparent transmission mode and strike the RRPP ring. Meantime, you must configure the 802.1p priority for trusted packets on the two ports accessing the RRPP ring.
- Do not configure the default VLAN of a port accessing an RRPP ring as the primary control VLAN or the secondary control VLAN, ensuring proper receiving/sending of RRPP packets.
- Do not enable QinQ or VLAN mapping on the control VLAN. Otherwise, RRPPDUs cannot be forwarded properly.
- You can still assign ports to or remove ports from the aggregation group corresponding to a Layer 2 aggregate interface configured as an RRPP port.

---

## Configuring Master Node

Follow these steps to configure master node:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an RRPP domain and enter its view | **rrpp domain** *domain-id* | Required |
| Specify control VLAN for the RRPP domain | **control-vlan** *vlan-id* | Required |
| Specify the protected VLANs for the RRPP domain | **protected-vlan reference-instance** *instance-id-list* | Required<br>No protected VLAN is specified for an RRPP domain by default. |
| Specify the current device as the master node of the ring, and specify the primary port and the secondary port | **ring** *ring-id* **node-mode master** [ **primary-port** *interface-type interface-number* ] [ **secondary-port** *interface-type interface-number* ] **level** *level-value* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the timer for the RRPP domain | **timer hello-timer** *hello-value* **fail-timer** *fail-value* | Optional<br>By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds. |
| Enable the RRPP ring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Return to system view | **quit** | — |
| Enable RRPP | **rrpp enable** | Required<br>By default, RRPP is disabled. |

**Caution**

- Before specifying RRPP rings for an RRPP domain, you must specify protected VLANs for the domain.
- Before specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- The **protected-vlan** command configures protected VLANs for an RRPP domain by referencing MSTIs to which the protected VLANs are mapped. You can use the **display stp region-configuration** command to view the VLAN-to-MSTI mappings. For detailed information about VLAN-to-MSTI mapping configuration, refer to *MSTP Configuration* in the *Access Volume*.
- The control VLAN configured for an RRPP domain must be a new one.
- Control VLAN configuration is required for configuring an RRPP ring.
- To use the **undo rrpp domain** command to remove an RRPP domain, you must ensure the RRPP domain has no RRPP ring.
- Before removing or modifying the control VLAN of an RRPP domain, make sure that the RRPP domain is not configured with any RRPP ring.

## Configuring Transit Node

Follow these steps to configure transit node:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an RRPP domain and enter its view | **rrpp domain** *domain-id* | Required |
| Specify a control VLAN for the RRPP domain | **control-vlan** *vlan-id* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify protected VLANs for the RRPP domain | **protected-vlan reference-instance** *instance-id-list* | Required<br>No protected VLAN is specified for an RRPP domain by default. |
| Specify the current device as the transit node of the ring, and specify the primary port and the secondary port | **ring** *ring-id* **node-mode transit** [ **primary-port** *interface-type interface-number* ] [ **secondary-port** *interface-type interface-number* ] **level** *level-value* | Required |
| Enable the RRPP ring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Return to system view | **quit** | — |
| Enable RRPP | **rrpp enable** | Required<br>By default, RRPP is disabled. |

**Caution**

- Before specifying RRPP rings for an RRPP domain, you must specify protected VLANs for the domain.
- Before specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- The **protected-vlan** command configures protected VLANs for an RRPP domain by referencing MSTIs to which the protected VLANs are mapped. You can use the **display stp region-configuration** command to view the VLAN-to-MSTI mappings. For detailed information about VLAN-to-MSTI mapping configuration, refer to *MSTP Configuration* in the *Access Volume*.
- The control VLAN configured for an RRPP domain must be a new one.
- Control VLAN configuration is required for configuring an RRPP ring.
- To use the **undo rrpp domain** command to remove an RRPP domain, you must ensure the RRPP domain has no RRPP ring.
- Before removing or modifying the control VLAN of an RRPP domain, make sure that the RRPP domain is not configured with any RRPP ring.

## Configuring Edge Node

Follow these steps to configure edge node:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an RRPP domain and enter its view | **rrpp domain** *domain-id* | Required |
| Specify a control VLAN for the RRPP domain | **control-vlan** *vlan-id* | Required |
| Specify protected VLANs for the RRPP domain | **protected-vlan reference-instance** *instance-id-list* | Required<br>No protected VLAN is specified for an RRPP domain by default. |
| Specify the current device as the transit node of the primary ring, and specify the primary port and the secondary port | **ring** *ring-id* **node-mode transit** [ **primary-port** *interface-type interface-number* ] [ **secondary-port** *interface-type interface-number* ] **level** *level-value* | Required |
| Specify the current device as the edge node of a subring, and specify the edge port | **ring** *ring-id* **node-mode edge** [ **edge-port** *interface-type interface-number* ] | Required |
| Enable the primary ring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Enable the subring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Return to system view | **quit** | — |
| Enable RRPP | **rrpp enable** | Required<br>By default, RRPP is disabled. |

**Caution**

- Before specifying RRPP rings for an RRPP domain, you must specify protected VLANs for the domain.
- Before specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- The **protected-vlan** command configures protected VLANs for an RRPP domain by referencing MSTIs to which the protected VLANs are mapped. You can use the **display stp region-configuration** command to view the VLAN-to-MSTI mappings. For detailed information about VLAN-to-MSTI mapping configuration, refer to *MSTP Configuration* in the *Access Volume*.
- The control VLAN configured for an RRPP domain must be a new one.
- Control VLAN configuration is required for configuring an RRPP ring.
- A Ring ID cannot be applied to more than one RRPP ring in an RRPP domain.
- You must first configure the primary ring and then the subring when configuring an edge node. Moreover, you must remove all subring configurations before deleting the primary ring configuration of an edge node. However, the RRPP ring enabled cannot be deleted.
- To use the **undo rrpp domain** command to remove an RRPP domain, you must ensure the RRPP domain has no RRPP ring.
- Before removing or modifying the control VLAN of an RRPP domain, make sure that the RRPP domain is not configured with any RRPP ring.

## Configuring Assistant Edge Node

Follow these steps to configure assistant-edge node:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an RRPP domain and enter its view | **rrpp domain** *domain-id* | Required |
| Specify a control VLAN for the RRPP domain | **control-vlan** *vlan-id* | Required |
| Specify protected VLANs for the RRPP domain | **protected-vlan reference-instance** *instance-id-list* | Required<br>No protected VLAN is specified for an RRPP domain by default. |
| Specify the current device as the transit node of the primary ring, and specify the primary port and the secondary port | **ring** *ring-id* **node-mode transit** [ **primary-port** *interface-type interface-number* ] [ **secondary-port** *interface-type interface-number* ] **level** *level-value* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify the current device as the assistant-edge node of the subring, and specify an edge port | **ring** *ring-id* **node-mode assistant-edge** [ **edge-port** *interface-type interface-number* ] | Required |
| Enable the primary ring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Enable the subring | **ring** *ring-id* **enable** | Required<br>By default, the RRPP ring is disabled. |
| Return to system view | **quit** | — |
| Enable RRPP | **rrpp enable** | Required<br>By default, RRPP is disabled. |

**Caution**

- Before specifying RRPP rings for an RRPP domain, you must specify protected VLANs for the domain.
- Before specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after specifying rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- The **protected-vlan** command configures protected VLANs for an RRPP domain by referencing MSTIs to which the protected VLANs are mapped. You can use the **display stp region-configuration** command to view the VLAN-to-MSTI mappings. For detailed information about VLAN-to-MSTI mapping configuration, refer to *MSTP Configuration* in the *Access Volume*.
- The control VLAN configured for an RRPP domain must be a new one.
- Control VLAN configuration is required for configuring an RRPP ring.
- A Ring ID cannot be applied to more than one RRPP ring in an RRPP domain.
- You must first configure the primary ring and then the subring when configuring an edge node. Moreover, you must remove all subring configurations before deleting the primary ring configuration of an edge node. However, the RRPP ring enabled cannot be deleted.
- To use the **undo rrpp domain** command to remove an RRPP domain, you must ensure the RRPP domain has no RRPP ring.
- Before removing or modifying the control VLAN of an RRPP domain, make sure that the RRPP domain is not configured with any RRPP ring.

## Configuring Ring Group

To reduce Edge-Hello traffic, you can adopt the ring group mechanism, that is, assign subrings with the same edge node/assistant-edge node to a ring group.

You need to configure ring groups on both the edge node and the assistant-edge node at the same time. The two ring groups must be configured with the same subrings. Otherwise, the ring groups cannot operate properly.

### Configuration Prerequisites

- The RRPP domain, control VLANs, protected VLANs, the primary ring, and the subrings have been configured on the edge node device.
- The RRPP domain, control VLANs, protected VLANs, the primary ring, and the subrings have been configured on the assistant-edge node device.

### Configuring Ring Group

Follow these steps to configure a ring group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a ring group and enter ring group view | **rrpp ring-group** *ring-group-id* | Required |
| Assign the specified subrings to the ring group | **domain** *domain-id* **ring** *ring-id-list* | Required |

**Note**

- To add an activated ring to a ring group, first add the ring to the assistant-edge node ring group and then to the edge node ring group.
- To remove a ring from a ring group, first remove the ring from the edge node ring group and then from the assistant-edge node group.
- To remove a ring group, first remove the edge node ring group and then the assistant-edge node ring group.
- To activate the rings in a ring group, first activate the rings in the assistant-edge node ring group and then the rings in the edge node ring group.
- To deactivate the rings in a ring group, first deactivate the rings in the edge node ring group and then the rings in the assistant-edge node ring group.
- If you do not following the orders above, the assistant-edge node may take the primary ring as failed because the assistant-edge node cannot receive Edge-Hello packets.

## Displaying and Maintaining RRPP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display brief information about RRPP configuration | **display rrpp brief** | Available in any view |
| Display detailed information about RRPP configuration | **display rrpp verbose domain** *domain-id* [ **ring** *ring-id* ] | |
| Display RRPP statistics | **display rrpp statistics domain** *domain-id* [ **ring** *ring-id* ] | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear RRPP statistics | **reset rrpp statistics domain** *domain-id* [ **ring** *ring-id* ] | Available in user view |

# RRPP Typical Configuration Examples

## Configuring Single Ring Topology

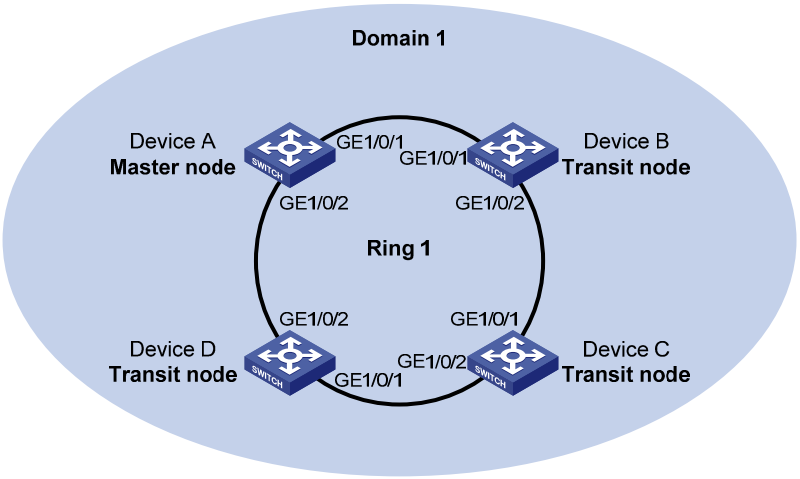
### Networking requirements

- Device A, Device B, Device C, and Device D constitute RRPP domain 1, specify the primary control VLAN of RRPP domain 1 as VLAN 4092, and RPPP domain 1 protects all VLANs;
- Device A, Device B, Device C and Device D constitute primary ring 1;
- Specify Device A as the master node of primary ring 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port;
- Specify Device B, Device C and Device D as the transit nodes of primary ring 1, their GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port;
- The timers of the primary ring adopt the default value.

First, determine the node mode of a device in an RRPP ring, and then perform the following configurations on a per-device basis:

- Disable STP on all ports accessing RRPP rings on these devices and configure these ports to permit the traffic of all VLANs to pass through.
- Configure the 802.1p priority for trusted packets on ports accessing RRPP rings on each device.
- Create an RRPP domain.
- Specify the control VLAN for the RRPP domain.
- Configure the MSTIs referenced by the protected VLANs. The MSTI ID ranges from 0 to 16.
- Specify the node mode of a device on the primary ring and the ports accessing the RRPP ring on the device.
- Enable the RRPP ring.
- Enable RRPP.

**Figure 1-8** Network diagram for single ring networking configuration



## Configuration procedure

1) Perform the following configuration on Device A:

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2) Perform the following configuration on Device B:

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3) Perform the following configuration on Device C:

The configuration on Device C is similar to that on Device B and thus omitted here.

4) Perform the following configuration on Device D:

The configuration on Device D is similar to that on Device B and thus omitted here.

5) Verification

After the above configuration, you can use the **display** command to view RRPP configuration on each device.

## Configuring Single-Domain Intersecting Ring Topology

### Networking requirements

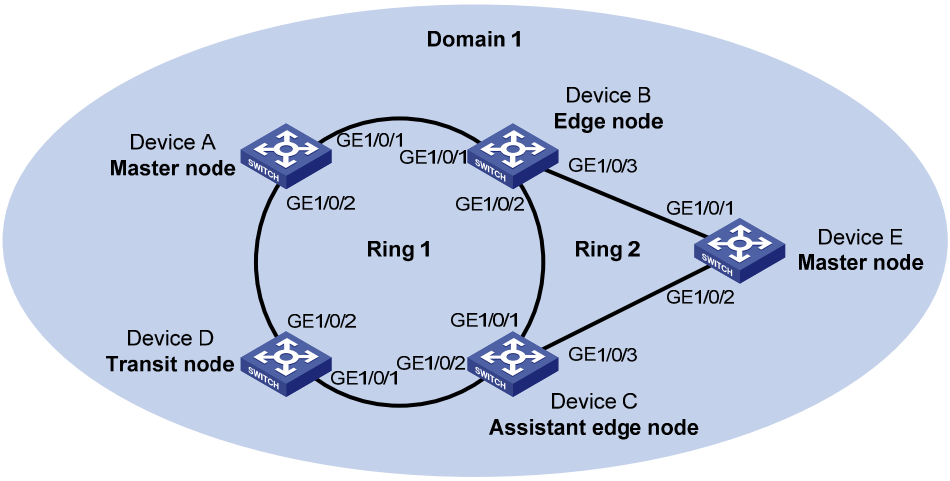
- Device A, Device B, Device C and Device D constitute RRPP domain 1, VLAN 4092 is the primary control VLAN of RRPP domain 1, and RRPP domain 1 protects all the VLANs;
- Device A, Device B, Device C and Device D constitute primary ring 1;
- Device B, Device C and Device E constitute subring 2;
- Device A is the master node of primary ring 1, GigabitEthernet 1/0/1 is the primary port and GigabitEthernet 1/0/2 is the secondary port;
- Device E is the master node of subring 2, GigabitEthernet 1/0/1 is the primary port and GigabitEthernet 1/0/2 is the secondary port;
- Device B is the transit node of primary ring 1 and the edge node of subring 2, and GigabitEthernet 1/0/3 is the edge port;
- Device C is the transit node of primary ring 1 and the assistant-edge node of subring 1, and GigabitEthernet 1/0/3 is the edge port;
- Device D is the transit node of primary ring 1, GigabitEthernet 1/0/1 is the primary port and GigabitEthernet 1/0/2 is the secondary port;
- The timers of both the primary ring and the subring adopt the default value.

First, determine the primary ring and subring in an RRPP domain, node mode of a device on each RRPP ring, and then perform the following configuration on a per-device basis:

- Disable STP on all ports accessing RRPP rings on these devices and configure these ports to permit the traffic of all VLANs to pass through.
- Configure the 802.1p priority for trusted packets on ports accessing RRPP rings on each device.
- Create an RRPP domain.

- Specify the control VLAN for the RRPP domain.
- Configure the protected VLANs to reference all MSTIs. The MSTI ID ranges from 0 to 16.
- Specify the node mode of a device on an RRPP ring and the ports accessing the RRPP ring on the device.
- Enable these two RRPP rings.
- Enable RRPP

**Figure 1-9** Network diagram for intersecting rings configuration




## Configuration procedure

1) Configuration on Device A

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2) Configuration on Device B

# Configure RRPP ports GigabitEthernet1/0/1, GigabitEthernet1/0/2 and GigabitEthernet1/0/3.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan all
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device B as a transit node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0//2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the edge node of subring 2, with GigabitEthernet1/0/3 as the edge port, and enable ring 2.

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3) Configuration on Device C

# Configure RRPP ports GigabitEthernet1/0/1, GigabitEthernet1/0/2 and GigabitEthernet1/0/3.

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan all
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 4092
[DeviceC-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device C as a transit node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

# Configure Device C as the assistant-edge node of subring 2, with GigabitEthernet1/0/3 as the edge port, and enable ring 2.

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

4) Configuration on Device D

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<DeviceD> system-view
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] quit
```

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 4092
[DeviceD-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device D as the transit node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

5) Configuration on Device E

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
<DeviceE> system-view
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan all
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan all
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTIs 0 through 16 as the protected VLANs of RRPP domain 1.

```
[DeviceE] rrpp domain 1
[DeviceE-rrpp-domain1] control-vlan 4092
[DeviceE-rrpp-domain1] protected-vlan reference-instance 0 to 16
```

# Configure Device E as the master node of subring 2, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceE] rrpp enable
```

6) Verification

After the configuration, you can use the **display** command to view RRPP configuration result on each device.

## Configuring Intersecting-Ring Load Balancing

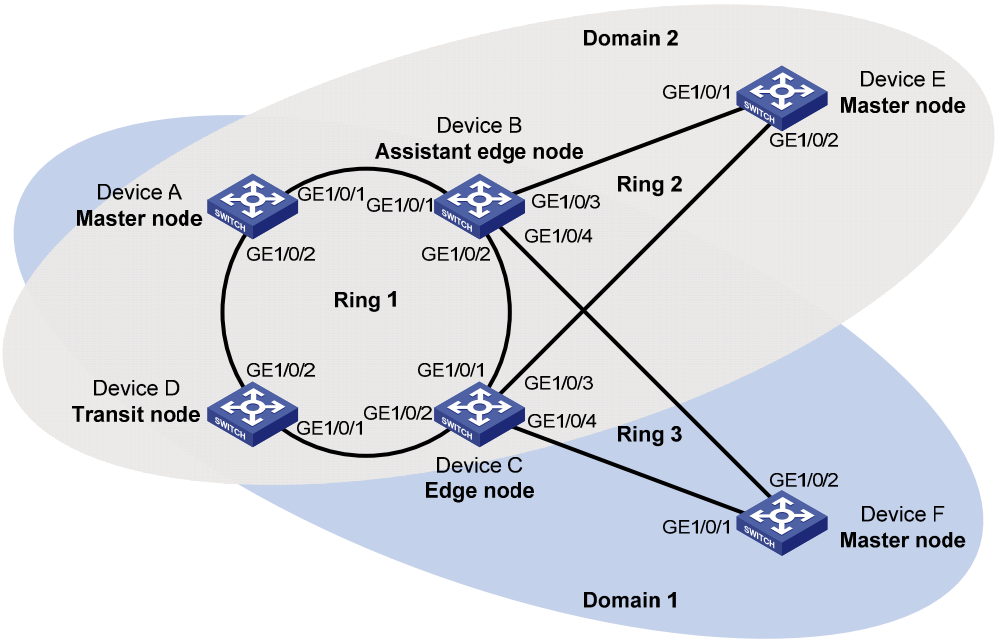
### Networking requirements

- Device A, Device B, Device C, Device D, and Device F constitute RRPP domain 1, and VLAN 100 is the primary control VLAN of the RRPP domain. Device A is the master node of the primary ring Ring 1; Device D is the transit node of the primary ring Ring 1; Device F is the master node of the subring Ring 3; Device C is the edge node of the subring Ring 3; Device B is the assistant-edge node of the subring Ring 3.
- Device A, Device B, Device C, Device D, and Device E constitute RRPP domain 2, and VLAN 105 is the primary control VLAN of the RRPP domain. Device A is the master node of the primary ring Ring 1; Device D is the transit node of the primary ring Ring 1; Device E is the master node of the subring Ring 2; Device C is the edge node of the subring Ring 2; Device B is the assistant-edge node of the subring Ring 2.
- Specify VLAN 10 as the protected VLAN of domain 1, and VLAN 20 as the protected VLAN of domain 2. Thus, you can achieve VLAN-based load balancing on the primary ring.
- As the edge node and assistant-edge node of subring Ring 2 is the same as those of subring Ring 3, and the two subrings have the same SRPTs, you can add subrings Ring 2 and Ring 3 to the RRPP ring group to reduce Edge-Hello traffic.

According to the diagram as shown Figure 1-10, perform the following configurations:

- Create data VLANs, and map the VLANs to be protected in each RRPP domain to different MSTIs.
- Disable STP on all ports accessing RRPP rings on these devices and configure the VLANs whose traffic is permitted to pass through.
- Configure the 802.1p priority for trusted packets on ports accessing RRPP rings on each device.
- Create RRPP domains.
- Specify control VLANs for RRPP domains.
- Specify protected VLANs for each domain by specifying MSTIs.
- Specify the roles of devices in these RRPP rings and the ports accessing RRPP rings.
- Enable RRPP rings.
- Enable the RRPP protocol.
- Configure a ring group on the edge nodes and assistant-edge nodes.

**Figure 1-10** Network diagram for intersecting-ring load balancing configuration




## Configuration procedure

1) Configure Device A as the master node of the primary ring

# Create VLANs 10 and 20, and map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] quit
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 20
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 100
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceA] rrpp domain 2
[DeviceA-rrpp-domain2] control-vlan 105
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet1/0/2 as the master port and GigabitEthernet1/0/1 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2 secondary-port gigabitethernet 1/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2) Configure Device B as the assistant-edge node of subrings Ring 2 and Ring 3

# Create VLANs 10 and 20, and map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 20
[DeviceB-vlan20] quit
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1, GigabitEthernet1/0/2, GigabitEthernet1/0/3, and GigabitEthernet1/0/4.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

```
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 20
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1, configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 100
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as a transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 3 in RRPP domain 1, with GigabitEthernet1/0/4 as the edge port, and enable subring 3.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceB] rrpp domain 2
[DeviceB-rrpp-domain2] control-vlan 105
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain2] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 2 in RRPP domain 2, with GigabitEthernet1/0/3 as the edge port, and enable subring 2.

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceB-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3) Configure Device C as the edge node of subrings Ring 2 and Ring 3

# Create VLANs 10 and 20, and map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 2 vlan 20
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1, GigabitEthernet1/0/2, GigabitEthernet1/0/3, and GigabitEthernet1/0/4.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 20
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface gigabitethernet 1/0/4
```

```
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 10
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1, configure VLAN 10 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 100
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device C as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

# Configure Device C as the edge node of subring 3 in RRPP domain 1, with GigabitEthernet1/0/4 as the edge port, and enable subring 3.

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceC] rrpp domain 2
[DeviceC-rrpp-domain2] control-vlan 105
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device C as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

# Configure Device C as the edge node of subring 2 in RRPP domain 2, with GigabitEthernet1/0/3 as the edge port, and enable subring 2.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

4) Configure Device D as a transit node of the primary ring

# Create VLANs 10 and 20, and map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.

```
<DeviceD> system-view
[DeviceD] vlan 10
[DeviceD-vlan10] quit
[DeviceD] vlan 20
```

```
[DeviceD-vlan20] quit
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 2 vlan 20
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 100
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device D as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN of RPPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceD] rrpp domain 2
[DeviceD-rrpp-domain2] control-vlan 105
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device D as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

5) Configure Device E as the master node of subring Ring 2 in domain 2

# Create VLAN 20, and map VLAN 20 to MSTI 2.

```
<DeviceE> system-view
[DeviceE] vlan 20
[DeviceE-vlan20] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 20
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 20
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 20
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN, and configure the VLAN mapped to MSTI 2 as the protected VLAN.

```
[DeviceE] rrpp domain 2
[DeviceE-rrpp-domain2] control-vlan 105
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device E as the master mode of subring 2 in RRPP domain 2, with GigabitEthernet1/0/2 as the primary port and GigabitEthernet1/0/1 as the secondary port, and enable ring 2.

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceE] rrpp enable
```

6) Configure Device F as the master node of subring Ring 3 in domain 1

# Create VLAN 10, and map VLAN 10 to MSTI 1.

```
<DeviceF> system-view
[DeviceF] vlan 10
[DeviceF-vlan10] quit
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 10
[DeviceF-mst-region] active region-configuration
```

```
[DeviceF-mst-region] quit
```

# Configure RRPP ports GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 10
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 10
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1, configure VLAN 100 as the primary control VLAN, and configure the VLAN mapped to MSTI 1 as the protected VLAN.

```
[DeviceF] rrpp domain 1
[DeviceF-rrpp-domain1] control-vlan 100
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device F as the master node of subring 3 in RRPP domain 1, with GigabitEthernet1/0/1 as the primary port and GigabitEthernet1/0/2 as the secondary port, and enable subring 3.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceF] rrpp enable
```

7) Configure a ring group on Device B and Device C after the configurations above

# Create RRPP ring group 1 on Device B, and add subrings 2 and 3 to the RRPP ring group.

```
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

# Create RRPP ring group 1 on Device C, and add subrings 2 and 3 to the RRPP ring group.

```
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3
```

8) Verification

After the configuration, you can use the **display** command to view RRPP configuration result on each device.

# Troubleshooting

**Symptom:**

When the link state is normal, the master node cannot receive Hello packets, and the master node unblocks the secondary port.

**Analysis:**

The reasons may be:

- RRPP is not enabled on some nodes in the RRPP ring.
- The domain ID or primary control VLAN ID is not the same for the nodes in the same RRPP ring.
- Some ports are abnormal.

**Solution:**

- Use the **display rrpp brief** command to check whether RRPP is enabled for all nodes. If not, use the **rrpp enable** command and the **ring enable** command to enable RRPP and RRPP rings for all nodes.
- Use the **display rrpp brief** command to check whether the domain ID and primary control VLAN ID are the same for all nodes. If not, set the same domain ID and primary control VLAN ID for the nodes.
- Use the **display rrpp verbose** command to check the link state of each port in each ring.
- Use the **debugging rrpp** command on each node to check whether a port receives or transmits Hello packets. If not, Hello packets are lost.

# Table of Contents

# 1 Port Mirroring Configuration

When configuring port mirroring, go to these sections for information you are interested in:



## Introduction to Port Mirroring

Port mirroring is to copy the packets passing through a port (called a mirroring port) to another port (called the monitor port) connected with a monitoring device for packet analysis.

You can select to port-mirror inbound, outbound, or bidirectional traffic on a port/VLAN as needed.

### Classification of Port Mirroring

Port mirroring can be local or remote.

- In local port mirroring, the mirroring port or ports and the monitor port are located on the same device.
- In remote port mirroring, the mirroring port or ports and the monitor port can be located on the same device or different devices. Currently, remote port mirroring can be implemented only at Layer 2.

---

**Note**

As a monitor port can monitor multiple ports, it may receive multiple duplicates of a packet in some cases. Suppose that port P 1 is monitoring bidirectional traffic on ports P 2 and P 3 on the same device. If a packet travels from P 2 to P 3, two duplicates of the packet will be received on P 1.

---

### Implementing Port Mirroring

Port mirroring is implemented through port mirroring groups. There are three types of mirroring groups: local, remote source, and remote destination.

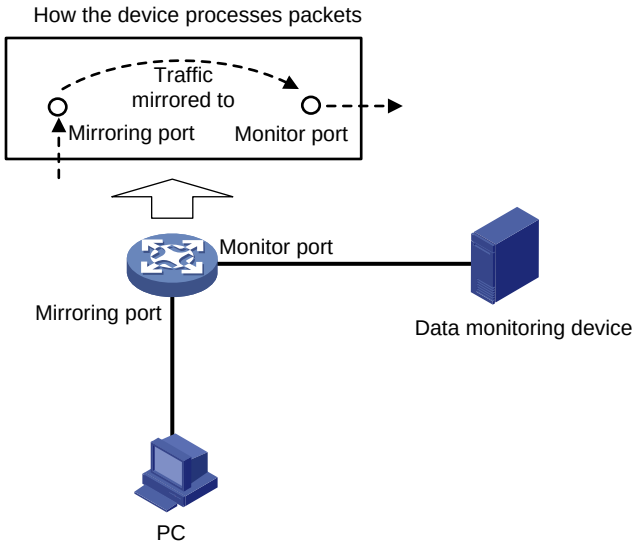
The following subsections describe how local port mirroring and remote port mirroring are implemented.

#### Local port mirroring

In local port mirroring, all packets passing through a port can be mirrored. Local port mirroring is implemented through a local mirroring group.

As shown in Figure 1-1, packets on the mirroring port are mirrored to the monitor port for the data monitoring device to analyze.

**Figure 1-1** Local port mirroring implementation

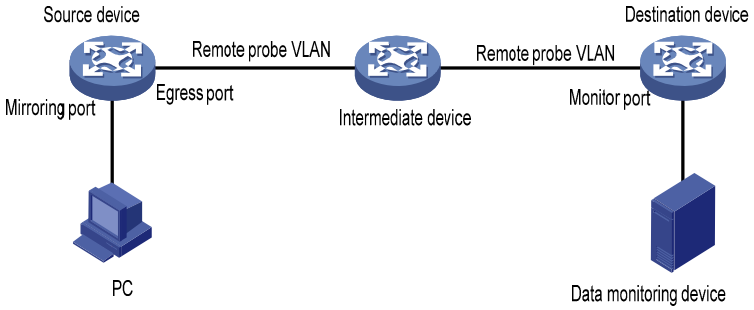



## Remote port mirroring

Remote port mirroring can mirror all packets but protocol packets.

Remote port mirroring is implemented through the cooperation of a remote source mirroring group and a remote destination mirroring group as shown Figure 1-2.

**Figure 1-2** Remote port mirroring implementation




Remote mirroring involves the following device roles:

- Source device

The source device is the device where the mirroring ports are located. On it, you must create a remote source mirroring group to hold the mirroring ports.

The source device copies the packets passing through the mirroring ports, broadcasts the packets in the remote probe VLAN for remote mirroring, and transmits the packets to the next device, which could be an intermediate device (if any) or the destination device.

- Intermediate device

Intermediate devices are devices located in between the source device and the destination device.

An intermediate device forwards mirrored packets to the next intermediate device (if any) or the destination device.

You must ensure that the source device and the destination device can communicate at Layer 2 in the remote probe VLAN.

- Destination device

The destination device is the device where the monitor port is located. On it, you must create the remote destination mirroring group.

When receiving a packet, the destination device compares the VLAN ID carried in the packet with the ID of the probe VLAN configured in the remote destination mirroring group. If they are the same, the device forwards the packet to the monitoring device through the monitor port.

**Note**

To make the port mirroring function work properly, before configuring bidirectional traffic mirroring on a port in a mirroring group, you need to use the **mac-address mac-learning disable** command on the source device, intermediate devices, and destination device to disable the MAC address learning function for the remote port mirroring VLAN. For more information about the **mac-address mac-learning disable** command, refer to *MAC Address Table Management Commands* in the *System Volume*.

## Configuring Local Port Mirroring

Configuring local port mirroring is to configure local mirroring groups.

A local mirroring group comprises one or multiple mirroring ports and one monitor port. These ports must not have been assigned to any other mirroring group.

Follow these steps to configure a local mirroring group:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a local mirroring group | | **mirroring-group** *groupid* **local** | Required |
| Configure mirroring ports | In system view | **mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **both** \| **inbound** \| **outbound** } | Required<br>You can configure mirroring ports in a mirroring group.<br>In system view, you can configure a list of mirroring ports to the mirroring group at a time.<br>In interface view, you can assign only the current port to the mirroring group. To monitor multiple ports, repeat the step. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | [ **mirroring-group** *groupid* ] **mirroring-port** { **both** \| **inbound** \| **outbound** } | |
| | | **quit** | |
| Configure the monitor port | In system view | **mirroring-group** *groupid* **monitor-port** *monitor-port-id* | Required<br>Use either approach. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | [ **mirroring-group** *groupid* ] **monitor-port** | |

Note

- A local port mirroring group takes effect only after its mirroring and monitor ports are configured.
- To ensure operation of your device, do not enable STP, MSTP, or RSTP on the monitor port.
- A port mirroring group can have multiple mirroring ports, but only one monitor port.
- A mirroring or monitor port to be configured cannot belong to an existing port mirroring group.
- You are recommended to use a monitor port only for port mirroring. This is to ensure that the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and normally forwarded traffic.

# Configuring Remote Port Mirroring

Configuring remote port mirroring is to configure remote mirroring groups. When doing that, configure the remote source mirroring group on the source device and the cooperating remote destination mirroring group on the destination device.

Note

If GVRP is enabled, GVRP may register the remote probe VLAN to unexpected ports, resulting in undesired duplicates. For information on GVRP, refer to *GVRP Configuration* in the *Access Volume*.

## Configuration Prerequisites

Create a static VLAN for the probe VLAN on the source and destination device. To ensure correct packet handling, ensure that the VLANs you created on the two devices use the same ID and function only for remote port mirroring.

## Configuring a Remote Source Mirroring Group (on the Source Device)

A remote source mirroring group comprises the following:

- One or multiple mirroring ports.
- A remote probe VLAN.
- An egress port.

After you assign a port to a mirroring group either as a mirroring port or as a monitor port, you cannot assign it to any other mirroring group. The same is true of probe VLANs.

### Configuring a remote source mirroring group with an egress port

Follow these steps to configure a remote port mirroring group with an egress port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a remote source mirroring group | **mirroring-group** *groupid* **remote-source** | Required |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure mirroring ports | In system view | **mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **both** \| **inbound** \| **outbound** } | Required<br>You configure multiple mirroring ports in a mirroring group.<br>In system view, you can assign a list of mirroring ports to the mirroring group at a time.<br>In interface view, you can assign only the current interface to the mirroring group. To monitor multiple ports, repeat the step. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | [ **mirroring-group** *groupid* ] **mirroring-port** { **both** \| **inbound** \| **outbound** } | |
| | | **quit** | |
| Configure the egress port | In system view | **mirroring-group** *groupid* **monitor-egress** *monitor-egress-port-id* | Required<br>Use either approach. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | **mirroring-group** *groupid* **monitor-egress** | |
| | | **quit** | |
| Configure the probe VLAN | | **mirroring-group** *groupid* **remote-probe vlan** *rprobe-vlan-id* | Required |

**Note**

When configuring the mirroring ports, note that:

- The mirroring ports and the egress port must be located on the same device.
- To ensure device performance, do not assign the mirroring ports to the remote probe VLAN.

**Note**

When configuring the egress port, note that:

- The port must not be a mirroring port in the mirroring group.
- To ensure operation of the device, disable these functions on the port: STP, MSTP, RSTP, 802.1X, IGMP Snooping, static ARP, and MAC address learning.
- A remote port mirroring group can have only one egress port.

**Note**

- To remove the VLAN configured as a remote probe VLAN, you must remove the remote probe VLAN with **undo mirroring-group remote-probe vlan** command first. Removing the probe VLAN can invalidate the remote source mirroring group.
- You are recommended to use a remote probe VLAN exclusively for the mirroring purpose.
- A port can belong to only one mirroring group. A VLAN can belong to only one mirroring group.

## Configuring a Remote Destination Mirroring Group (on the Destination Device)

A remote destination mirroring group comprises a remote probe VLAN and a monitor port. You must ensure that the remote probe VLAN is the same as the one configured in the remote source mirroring group.

Follow these steps to configure a remote destination port mirroring group:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a remote destination mirroring group | | **mirroring-group** *groupid* **remote-destination** | Required |
| Configure the remote probe VLAN | | **mirroring-group** *groupid* **remote-probe vlan** *rprobe-vlan-id* | Required |
| Configure the monitor port | In system view | **mirroring-group** *groupid* **monitor-port** *monitor-port-id* | Required<br>Use either approach. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | [ **mirroring-group** *groupid* ] **monitor-port** | |
| | | **quit** | |
| Enter the interface view of the monitor port | | **interface** *interface-type interface-number* | — |
| Assign the port to the probe VLAN | For an access port | **port access vlan** *rprobe-vlan-id* | Required<br>Use one of the commands depending on the link type of the monitor port. |
| | For a trunk port | **port trunk permit vlan** *rprobe-vlan-id* | |
| | For a hybrid port | **port hybrid vlan** *rprobe-vlan-id* { **tagged** \| **untagged** } | |

**Note**

When configuring the probe VLAN, use the following guidelines:

- A VLAN can be the remote probe VLAN of only one port mirroring group.
- To remove the VLAN configured as the remote probe VLAN, you must remove the remote probe VLAN with **undo mirroring-group remote-probe vlan** command first. Removing the probe VLAN can invalidate the remote source mirroring group.

**Note**

When configuring the monitor port, use the following guidelines:

- The port can belong to only the current mirroring group.
- To ensure operation of your device, do not assign the monitor port to a mirroring VLAN.
- Disable these functions on the port: STP, MSTP, and RSTP.
- You are recommended to use a monitor port only for port mirroring. This is to ensure that the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and normally forwarded traffic.

# Displaying and Maintaining Port Mirroring

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration of port mirroring groups | **display mirroring-group** { *groupid* \| **all** \| **local** \| **remote-destination** \| **remote-source** } | Available in any view |

# Port Mirroring Configuration Examples

## Local Port Mirroring Configuration Example

### Network requirements

The departments of a company connect to each other through Ethernet switches:

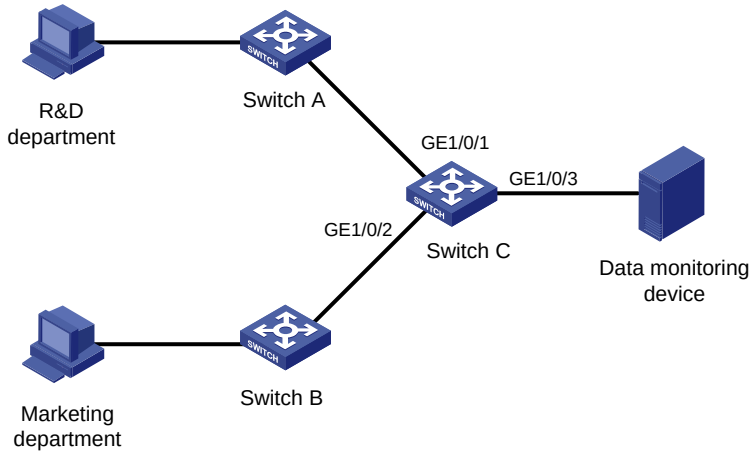
- Research and Development (R&D) department is connected to Switch C through GigabitEthernet 1/0/1.
- Marketing department is connected to Switch C through GigabitEthernet 1/0/2.
- Data monitoring device is connected to Switch C through GigabitEthernet 1/0/3

As shown in Figure 1-3, the administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data monitoring device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as mirroring source ports.
- Configure GigabitEthernet 1/0/3 as the mirroring destination port.

**Figure 1-3** Network diagram for local port mirroring configuration




### Configuration procedure

Configure Switch C.

# Create a local port mirroring group.

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
```

# Add port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the port mirroring group as source ports. Add port GigabitEthernet 1/0/3 to the port mirroring group as the destination port.

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 both
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

# Display the configuration of all the port mirroring groups.

```
[SwitchC] display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
        GigabitEthernet1/0/2  both
    monitor port: GigabitEthernet1/0/3
```

After finishing the configuration, you can monitor all the packets received and sent by R&D department and Marketing department on the Data monitoring device.

## Remote Port Mirroring Configuration Example

### Network requirements

The departments of a company connect to each other through Ethernet switches:

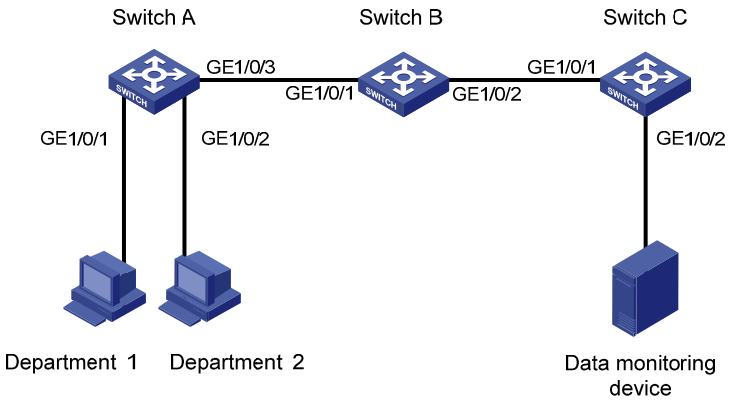
- Department 1 is connected to GigabitEthernet 1/0/1 of Switch A.
- Department 2 is connected to GigabitEthernet 1/0/2 of Switch A.
- GigabitEthernet 1/0/3 of Switch A connects to GigabitEthernet 1/0/1 of Switch B.
- GigabitEthernet 1/0/2 of Switch B connects to GigabitEthernet 1/0/1 of Switch C.
- The data monitoring device is connected to GigabitEthernet 1/0/2 of Switch C.

As shown in Figure 1-4, the administrator wants to monitor the packets sent from Department 1 and 2 through the data monitoring device.

Use the remote port mirroring function to meet the requirement. Perform the following configurations:

- Use Switch A as the source device, Switch B as the intermediate device, and Switch C as the destination device.
- On Switch A, create a remote source mirroring group; create VLAN 2 and configure it as the remote port mirroring VLAN; add port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the port mirroring group as two source ports. Configure port GigabitEthernet 1/0/3 as the outbound mirroring port.
- Configure port GigabitEthernet 1/0/3 of Switch A, port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B, and port GigabitEthernet 1/0/1 of Switch C as trunk ports and configure them to permit packets of VLAN 2.
- Create a remote destination mirroring group on Switch C. Configure VLAN 2 as the remote port mirroring VLAN and port GigabitEthernet 1/0/2, to which the data monitoring device is connected, as the destination port.

**Figure 1-4** Network diagram for remote port mirroring configuration




## Configuration procedure

1) Configure Switch A (the source device).

# Create a remote source port mirroring group.

```
<SwitchA> system-view
[SwitchA] mirroring-group 1 remote-source
```

# Create VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

# Configure VLAN 2 as the remote port mirroring VLAN of the remote port mirroring group. Add port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the remote port mirroring group as source ports. Configure port GigabitEthernet 1/0/3 as the outbound mirroring port.

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
inbound
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/3
```

# Configure port GigabitEthernet 1/0/3 as a trunk port and configure the port to permit the packets of VLAN 2.

```
[SwitchA] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
```

2) Configure Switch B (the intermediate device).

# Configure port GigabitEthernet 1/0/1 as a trunk port and configure the port to permit the packets of VLAN 2.

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

# Configure port GigabitEthernet 1/0/2 as a trunk port and configure the port to permit the packets of VLAN 2.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
```

3) Configure Switch C (the destination device).

# Configure port GigabitEthernet 1/0/1 as a trunk port and configure the port to permit the packets of VLAN 2.

```
<SwitchC> system-view
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/1] quit
```

# Create a remote destination port mirroring group.

```
[SwitchC] mirroring-group 1 remote-destination
```

# Create VLAN 2.

```
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

# Configure VLAN 2 as the remote port mirroring VLAN of the remote destination port mirroring group. Add port GigabitEthernet 1/0/2 to the remote destination port mirroring group as the destination port.

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 2
```

After finishing the configuration, you can monitor all the packets sent by Department 1 and Department 2 on the Data monitoring device.

# IP Services Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The IP Services Volume is organized as follows:

| Features | Description |
|---|---|
| IP Address | An IP address is a 32-bit address allocated to a network interface on a device that is attached to the Internet. This document describes:<br>• Introduction to IP addresses<br>• IP address configuration |
| ARP | Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address. This document describes:<br>• ARP Overview<br>• Configuring ARP<br>• Configuring Gratuitous ARP<br>• Proxy ARP and Local Proxy ARP configuration<br>• ARP Attack Defense configuration |
| DHCP | DHCP is built on a client-server model, in which the client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client. This document describes:<br>• DHCP relay agent configuration<br>• DHCP Client configuration<br>• DHCP Snooping configuration<br>• BOOTP Client configuration |
| DNS | Used in the TCP/IP application, Domain Name System (DNS) is a distributed database which provides the translation between domain name and the IP address. This document describes:<br>• Configuring the DNS Client<br>• Configuring the DNS Proxy |
| IP Performance | In some network environments, you need to adjust the IP parameters to achieve best network performance. This document describes:<br>• Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network<br>• Configuring TCP Attributes<br>• Configuring ICMP to Send Error Packets |

| Features | Description |
| --- | --- |
| UDP Helper | UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified server. This document describes:<br>• UDP Helper overview<br>• UDP Helper configuration |
| IPv6 Basics | Internet protocol version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet protocol version 4 (IPv4). This document describes:<br>• IPv6 overview<br>• Basic IPv6 functions configuration<br>• IPv6 NDP configuration<br>• PMTU discovery configuration<br>• IPv6 TCP properties configuration<br>• ICMPv6 packet sending configuration<br>• IPv6 DNS Client configuration |
| Dual Stack | A network node that supports both IPv4 and IPv6 is called a dual stack node. A dual stack node configured with an IPv4 address and an IPv6 address can have both IPv4 and IPv6 packets transmitted. This document describes:<br>• Dual stack overview<br>• Dual stack configuration |
| sFlow | Based on packet sampling, Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics. This document describes:<br>• sFlow Overview<br>• sFlow Configuration |

# Table of Contents

# 1 IP Addressing Configuration

When assigning IP addresses to interfaces on your device, go to these sections for information you are interested in:

- IP Addressing Overview
- Configuring IP Addresses
- Displaying and Maintaining IP Addressing

## IP Addressing Overview

This section covers these topics:

- IP Address Classes
- Special IP Addresses

### IP Address Classes

On an IP network, a 32-bit address is used to identify a host. An example is 01010000100000001000000010000000 in binary. To make IP addresses in 32-bit form easier to read, they are written in dotted decimal notation, each being four octets in length, for example, 10.1.1.1 for the address just mentioned.

Each IP address breaks down into two parts:

- Net ID: The first several bits of the IP address defining a network, also known as class bits.
- Host-id: Identifies a host on a network.

IP addresses are divided into five classes, as shown in the following figure (in which the blue parts represent the address class).

**Figure 1-1** IP address classes

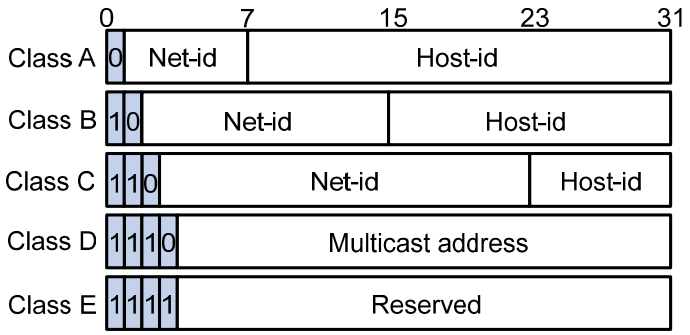



Table 1-1 describes the address ranges of these five classes.

**Table 1-1** IP address classes and ranges

| Class | Address range | Remarks |
|---|---|---|
| A | 0.0.0.0 to 127.255.255.255 | The IP address 0.0.0.0 is used by a host at bootstrap for temporary communication. This address is never a valid destination address.<br>Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link. |
| B | 128.0.0.0 to 191.255.255.255 | — |
| C | 192.0.0.0 to 223.255.255.255 | — |
| D | 224.0.0.0 to 239.255.255.255 | Multicast addresses. |
| E | 240.0.0.0 to 255.255.255.255 | Reserved for future use except for the broadcast address 255.255.255.255. |

## Special IP Addresses

The following IP addresses are for special use, and they cannot be used as host IP addresses:

- IP address with an all-zero net ID: Identifies a host on the local network. For example, IP address 0.0.0.16 indicates the host with a host ID of 16 on the local network.
- IP address with an all-zero host ID: Identifies a network.
- IP address with an all-one host ID: Identifies a directed broadcast address. For example, a packet with the destination address of 192.168.1.255 will be broadcasted to all the hosts on the network 192.168.1.0.

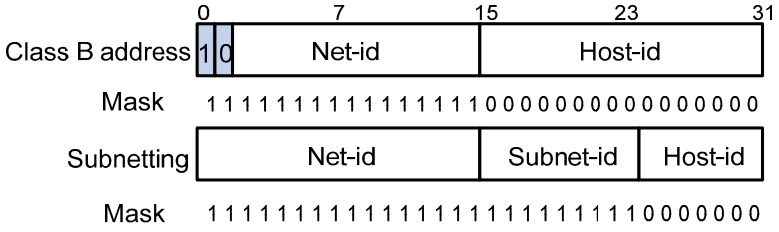
## Subnetting and Masking

Subnetting was developed to address the risk of IP address exhaustion resulting from fast expansion of the Internet. The idea is to break a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID. To identify the boundary between the host ID and the combination of net ID and subnet ID, masking is used.

Each subnet mask comprises 32 bits related to the corresponding bits in an IP address. In a subnet mask, the part containing consecutive ones identifies the combination of net ID and subnet ID whereas the part containing consecutive zeros identifies the host ID.

Figure 1-2 shows how a Class B network is subnetted.

**Figure 1-2** Subnet a Class B network



In the absence of subnetting, some special addresses such as the addresses with the net ID of all zeros and the addresses with the host ID of all ones, are not assignable to hosts. The same is true for subnetting. When designing your network, you should note that subnetting is somewhat a tradeoff between subnets and accommodated hosts. For example, a Class B network can accommodate 65,534 ($2^{16}$ – 2. Of the two deducted Class B addresses, one with an all-one host ID is the broadcast address and the other with an all-zero host ID is the network address) hosts before being subnetted. After you break it down into 512 ($2^9$) subnets by using the first 9 bits of the host ID for the subnet, you have only 7 bits for the host ID and thus have only 126 ($2^7$ – 2) hosts in each subnet. The maximum number of hosts is thus 64,512 (512 × 126), 1022 less after the network is subnetted.

Class A, B, and C networks, before being subnetted, use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

# Configuring IP Addresses

An interface needs an IP address to communicate with other devices. You can assign an IP address to a VLAN interface or a loopback interface on a switch. Besides directly assigning an IP address to the VLAN interface, you may configure the VLAN interface to obtain one through BOOTP, or DHCP as alternatives. If you change the way an interface obtains an IP address, from manual assignment to BOOTP for example, the IP address obtained from BOOTP will overwrite the old one manually assigned.

---

 **Note**

This chapter only covers how to assign an IP address manually. For the other two approaches, refer to *DHCP Configuration* in the *IP Services Volume*.

---

This section includes:



## Assigning an IP Address to an Interface

You may assign an interface on the switch multiple IP addresses, one primary and multiple secondaries, to connect multiple logical subnets on the same physical subnet.

Follow these steps to assign an IP address to an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Assign an IP address to the interface | **ip address** *ip-address* { *mask* \| *mask-length* } [ **sub** ] | Required<br>No IP address is assigned by default. |

**Caution**

- The primary IP address you assigned to the interface can overwrite the old one if there is any.
- You cannot assign secondary IP addresses to an interface that has BOOTP or DHCP configured.
- The primary and secondary IP addresses you assign to the interface can be located on the same network segment. However, this should not violate the rule that different physical interfaces on your device must reside on different network segments.

## IP Addressing Configuration Example

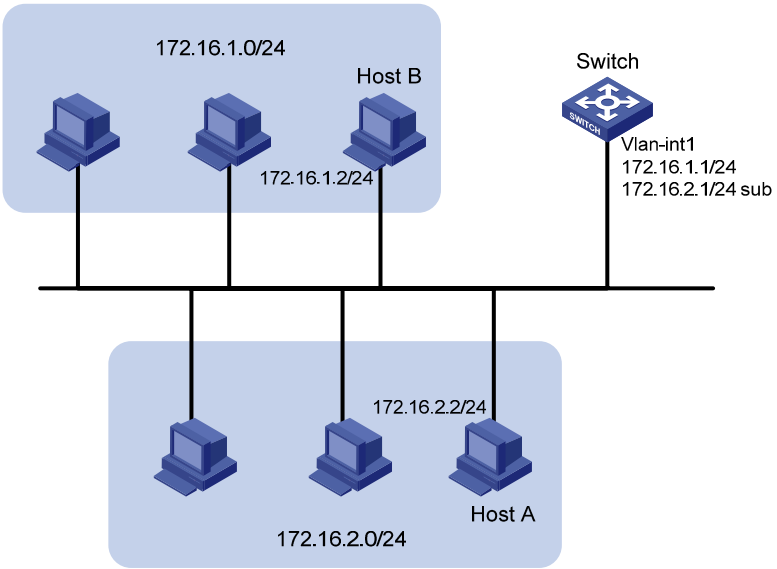
### Network requirements

As shown in Figure 1-3, a port in VLAN 1 on a switch is connected to a LAN comprising two segments: 172.16.1.0/24 and 172.16.2.0/24.

To enable the hosts on the two network segments to communicate with the external network through the switch, and the hosts on the LAN can communicate with each other, do the following:

- Assign two IP addresses to VLAN-interface 1 on the switch.
- Set the switch as the gateway on all PCs in the two networks.

**Figure 1-3** Network diagram for IP addressing configuration




### Configuration procedure

# Assign a primary IP address and a secondary IP address to VLAN-interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
```

# Set the gateway address to 172.16.1.1 on the PCs attached to subnet 172.16.1.0/24, and to 172.16.2.1 on the PCs attached to subnet 172.16.2.0/24.

# Ping a host on subnet 172.16.1.0/24 from the switch to check the connectivity.

```
<Switch> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

The output information shows that the switch can communicate with the hosts on subnet 172.16.1.0/24.

# Ping a host on subnet 172.16.2.0/24 from the switch to check the connectivity.

```
<Switch> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

The output information shows that the switch can communicate with the hosts on subnet 172.16.2.0/24.

# Ping a host on subnet 172.16.1.0/24 from a host on subnet 172.16.2.0/24 to check the connectivity. Host B can be successfully pinged from Host A.

## Displaying and Maintaining IP Addressing

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about a specified or all Layer 3 interfaces | **display ip interface** [ *interface-type interface-number* ] | Available in any view |
| Display brief information about a specified or all Layer 3 interfaces | **display ip interface brief** [ *interface-type* [ *interface-number* ] ] | |

# Table of Contents

This document is organized as follows:



# 1 ARP Configuration

When configuring ARP, go to these sections for information you are interested in:



## ARP Overview

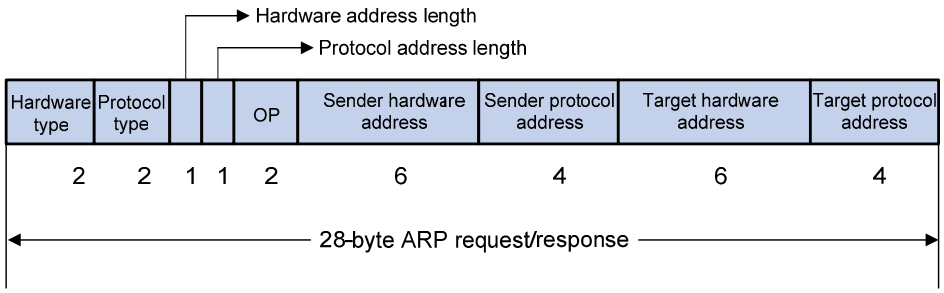
### ARP Function

The Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address (or physical address).

In a LAN, when a host or other network device is to send data to another host or device, the sending host or device must know the network layer address (that is, the IP address) of the destination host or device. Because IP datagrams must be encapsulated within Ethernet frames before they can be transmitted over physical networks, the sending host or device also needs to know the physical address of the destination host or device. Therefore, a mapping between the IP address and the physical address is needed. ARP is the protocol to implement the mapping function.

### ARP Message Format

**Figure 1-1** ARP message format




The following explains the fields in Figure 1-1.

- Hardware type: This field specifies the hardware address type. The value “1” represents Ethernet.
- Protocol type: This field specifies the type of the protocol address to be mapped. The hexadecimal value “0x0800” represents IP.

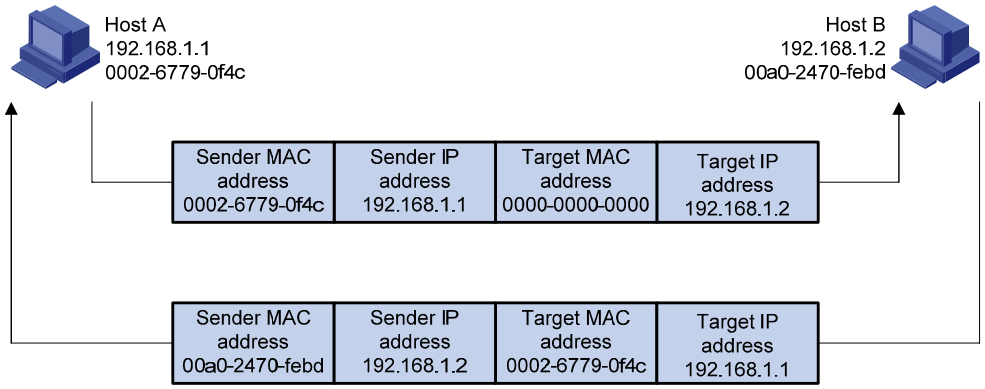
- Hardware address length and protocol address length: They respectively specify the length of a hardware address and a protocol address, in bytes. For an Ethernet address, the value of the hardware address length field is "6". For an IP(v4) address, the value of the protocol address length field is "4".
- OP: Operation code. This field specifies the type of ARP message. The value "1" represents an ARP request and "2" represents an ARP reply.
- Sender hardware address: This field specifies the hardware address of the device sending the message.
- Sender protocol address: This field specifies the protocol address of the device sending the message.
- Target hardware address: This field specifies the hardware address of the device the message is being sent to.
- Target protocol address: This field specifies the protocol address of the device the message is being sent to.

## ARP Address Resolution Process

Suppose that Host A and Host B are on the same subnet and Host A sends a packet to Host B, as shown in Figure 1-2. The resolution process is as follows:

1) Host A looks into its ARP table to see whether there is an ARP entry for Host B. If yes, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
2) If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the sender IP address and the sender MAC address are the IP address and the MAC address of Host A respectively, and the target IP address and the target MAC address are the IP address of Host B and an all-zero MAC address respectively. Because the ARP request is a broadcast, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will respond to the request.
3) Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address in its ARP table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
4) After receiving the ARP reply, Host A adds the MAC address of Host B to its ARP table. Meanwhile, Host A encapsulates the IP packet and sends it out.

**Figure 1-2** ARP address resolution process




If Host A is not on the same subnet with Host B, Host A first sends an ARP request to the gateway. The target IP address in the ARP request is the IP address of the gateway. After obtaining the MAC address

of the gateway from an ARP reply, Host A sends the packet to the gateway. If the gateway maintains the ARP entry of Host B, it forwards the packet to Host B directly; if not, it broadcasts an ARP request, in which the target IP address is the IP address of Host B. After obtaining the MAC address of Host B, the gateway sends the packet to Host B.

## ARP Table

After obtaining the MAC address for the destination host, the device puts the IP-to-MAC mapping into its own ARP table. This mapping is used for forwarding packets with the same destination in future.

An ARP table contains ARP entries, which fall into one of two categories: dynamic or static.

### Dynamic ARP entry

A dynamic entry is automatically created and maintained by ARP. It can get aged, be updated by a new ARP packet, or be overwritten by a static ARP entry. When the aging timer expires or the interface goes down, the corresponding dynamic ARP entry will be removed.

### Static ARP entry

A static ARP entry is manually configured and maintained. It cannot get aged or be overwritten by a dynamic ARP entry.

Using static ARP entries enhances communication security. You can configure a static ARP entry to restrict an IP address to communicate with the specified MAC address only. After that, attack packets cannot modify the IP-to-MAC mapping specified in the static ARP entry. Thus, communications between the protected device and the specified device are ensured.

Static ARP entries can be classified into permanent or non-permanent.

- A permanent static ARP entry can be directly used to forward packets. When configuring a permanent static ARP entry, you must configure a VLAN and an outbound interface for the entry besides the IP address and the MAC address.
- A non-permanent static ARP entry has only an IP address and a MAC address configured. If a non-permanent static ARP entry matches an IP packet to be forwarded, the device sends an ARP request first. If the sender IP and MAC addresses in the received ARP reply are the same as those in the non-permanent static ARP entry, the device adds the interface receiving the ARP reply to the non-permanent static ARP entry. Then the entry can be used for forwarding IP packets.

---

 **Note**

Usually ARP dynamically resolves IP addresses to MAC addresses, without manual intervention.

---

# Configuring ARP

## Configuring a Static ARP Entry

A static ARP entry is effective when the device works normally. However, when a VLAN or VLAN interface to which a static ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved.

Follow these steps to configure a static ARP entry:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a permanent static ARP entry | **arp static** *ip-address mac-address vlan-id interface-type interface-number* | Required<br>No permanent static ARP entry is configured by default. |
| Configure a non-permanent static ARP entry | **arp static** *ip-address mac-address* | Required<br>No non-permanent static ARP entry is configured by default. |

**Caution**

The *vlan-id* argument must be the ID of an existing VLAN which corresponds to the ARP entries. In addition, the Ethernet interface following the argument must belong to that VLAN. A VLAN interface must be created for the VLAN.

## Configuring the Maximum Number of ARP Entries for a Interface

Follow these steps to set the maximum number of dynamic ARP entries that a interface can learn:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Set the maximum number of dynamic ARP entries that a interface can learn | **arp max-learning-num** *number* | Optional<br>2048 by default. |

## Setting the Aging Time for Dynamic ARP Entries

To keep pace with the network changes, the ARP table is refreshed. Each dynamic ARP entry in the ARP table has a limited lifetime rather than is always valid. Dynamic ARP entries that are not refreshed before expiring are deleted from the ARP table. The lifetime is called the aging time. The aging time is reset each time the dynamic ARP entry is used within the lifetime. You can adjust the aging time for dynamic ARP entries according to the actual network condition.

Follow these steps to set the aging time for dynamic ARP entries:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the aging time for dynamic ARP entries | **arp timer aging** *aging-time* | Optional<br>20 minutes by default. |

## Enabling the ARP Entry Check

The ARP entry check function disables the device from learning multicast MAC addresses. With the ARP entry check enabled, the device cannot learn any ARP entry with a multicast MAC address, and configuring such a static ARP entry is not allowed; otherwise, the system displays error messages.

After the ARP entry check is disabled, the device can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the device.

Follow these steps to enable the ARP entry check:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the ARP entry check | **arp check enable** | Optional<br>By default, the device is disabled from learning multicast MAC addresses. |

## ARP Configuration Example

### Network requirements

- Enable the ARP entry check.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Set the maximum number of dynamic ARP entries that VLAN-interface 10 can learn to 1,000.
- Add a static ARP entry, with the IP address being 192.168.1.1/24, the MAC address being 000f-e201-0000, and the outbound interface being GigabitEthernet 1/0/1 of VLAN 10.

### Configuration procedure

```
<Sysname> system-view
[Sysname] arp check enable
[Sysname] arp timer aging 10
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 10
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface vlan-interface 10
[Sysname-vlan-interface10] arp max-learning-num 1000
[Sysname-vlan-interface10] quit
[Sysname] arp static 192.168.1.1 000f-e201-0000 10 gigabitethernet 1/0/1
```

# Configuring Gratuitous ARP

## Introduction to Gratuitous ARP

A gratuitous ARP packet is a special ARP packet, in which the sender IP address and the target IP address are both the IP address of the sender, the sender MAC address is the MAC address of the sender, and the target MAC address is the broadcast address ff:ff:ff:ff:ff:ff.

A device implements the following functions by sending gratuitous ARP packets:

- Determining whether its IP address is already used by another device.
- Informing other devices of its MAC address change so that they can update their ARP entries.

A device receiving a gratuitous ARP packet adds the information carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry for the ARP packet in the cache.

### Configuring Gratuitous ARP

Follow these steps to configure gratuitous ARP:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the device to send gratuitous ARP packets when receiving ARP requests from another network segment | **gratuitous-arp-sending enable** | Required<br>By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment. |
| Enable the gratuitous ARP packet learning function | **gratuitous-arp-learning enable** | Optional<br>Enabled by default. |

## Displaying and Maintaining ARP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display ARP entries in the ARP table | **display arp** [ [ **all** \| **dynamic** \| **static** ] \| **vlan** *vlan-id* \| **interface** *interface-type interface-number* ] [ [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] \| **count** ] | Available in any view |
| Display the ARP entry for a specified IP address | **display arp** *ip-address* [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | Available in any view |
| Display the aging time for dynamic ARP entries | **display arp timer aging** | Available in any view |
| Clear ARP entries from the ARP table<br>For distributed devices | **reset arp** { **all** \| **dynamic** \| **static** \| **interface** *interface-type interface-number* } | Available in user view |

# 2 Proxy ARP Configuration

When configuring proxy ARP, go to these sections for information you are interested in:

- Proxy ARP Overview
- Enabling Proxy ARP
- Displaying and Maintaining Proxy ARP

## Proxy ARP Overview

If a host sends an ARP request for the MAC address of another host that actually resides on another network (but the sending host considers the requested host is on the same network) or that is isolated from the sending host at Layer 2, the device in between must be able to respond to the request with the MAC address of the receiving interface to allow Layer 3 communication between the two hosts. This is achieved by proxy ARP. Proxy ARP hides the physical details of the network.

Proxy ARP involves common proxy ARP and local proxy ARP, which are described in the following sections.

**Note**

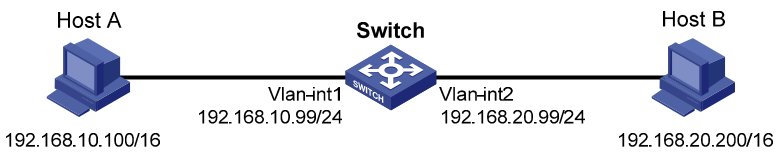
The term proxy ARP in the following sections of this chapter refers to common proxy ARP unless otherwise specified.

### Proxy ARP

A proxy ARP enabled device allows hosts that reside on different subnets to communicate.

As shown in Figure 2-1, Switch connects to two subnets through VLAN-interface 1 and VLAN-interface 2. The IP addresses of the two interfaces are 192.168.10.99/24 and 192.168.20.99/24. Host A and Host B have the same prefix 192.168.0.0 assigned and connect to VLAN-interface 1 and VLAN-interface 2, respectively.

**Figure 2-1** Application environment of proxy ARP




Because Host A considers that Host B is on the same network, it directly sends an ARP request for the MAC address of Host B. Host B, however, cannot receive this request because it locates in a different broadcast domain.

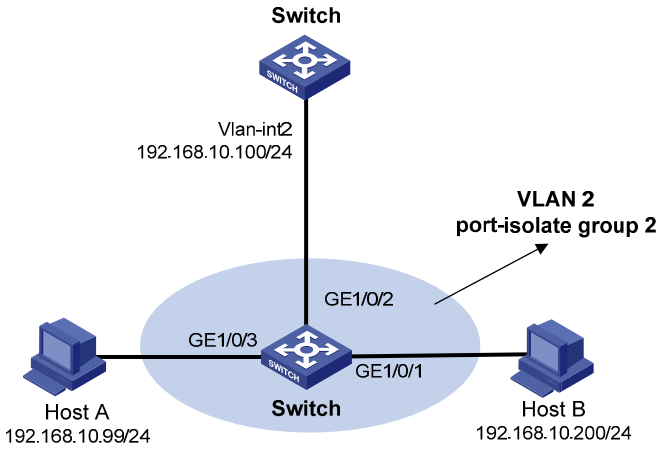
You can solve the problem by enabling proxy ARP on Switch. After that, Switch can reply to the ARP request from Host A with the MAC address of VLAN-interface 1, and forward packets sent from Host A to Host B. In this case, Switch seems to be a proxy of Host B.

A main advantage of proxy ARP is that it is added on a single router without disturbing routing tables of other routers in the network. Proxy ARP acts as the gateway for IP hosts that are not configured with a default gateway or do not have routing capability.

### Local Proxy ARP

As shown in Figure 2-2, Host A and Host B belong to VLAN 2, but are isolated at Layer 2. Host A connects to GigabitEthernet 1/0/3 while Host B connects to GigabitEthernet 1/0/1. Enable local proxy ARP on Switch to allow Layer 3 communication between the two hosts.

**Figure 2-2** Application environment of local proxy ARP




In one of the following cases, you need to enable local proxy ARP:

- Hosts connecting to different isolated Layer 2 ports in the same VLAN need to communicate at Layer 3.
- If an isolate-user-vlan is configured, hosts in different secondary VLANs of the isolate-user-vlan need to communicate at Layer 3.

## Enabling Proxy ARP

Follow these steps to enable proxy ARP in VLAN interface view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Required |
| Enable proxy ARP | **proxy-arp enable** | Required<br>Disabled by default. |

Follow these steps to enable local proxy ARP in VLAN interface view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable local proxy ARP | **local-proxy-arp enable** | Required<br>Disabled by default. |

# Displaying and Maintaining Proxy ARP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display whether proxy ARP is enabled | **display proxy-arp** [ **interface vlan-interface** *vlan-id* ] | Available in any view |
| Display whether local proxy ARP is enabled | **display local-proxy-arp** [ **interface vlan-interface** *vlan-id* ] | Available in any view |

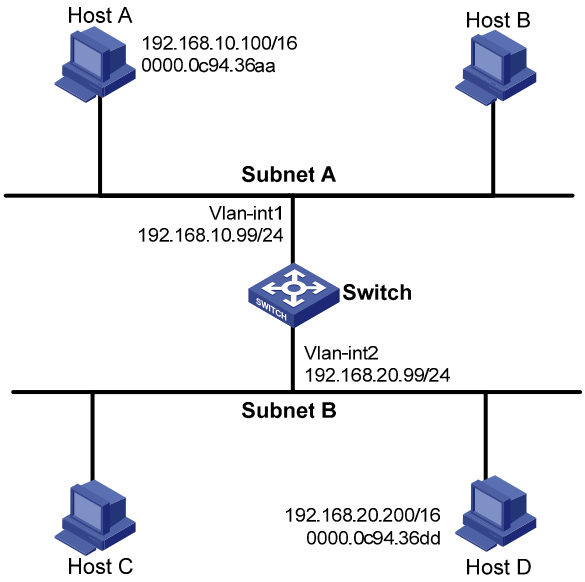
# Proxy ARP Configuration Examples

## Proxy ARP Configuration Example

### Network requirements

Host A and Host D have the same IP prefix and mask. Host A belongs to VLAN 1; Host D belongs to VLAN 2. Configure proxy ARP on the switch to enable the communication between the two hosts.

**Figure 2-3** Network diagram for proxy ARP




### Configuration procedure

# Configure Proxy ARP on Switch to enable the communication between Host A and Host D.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
```

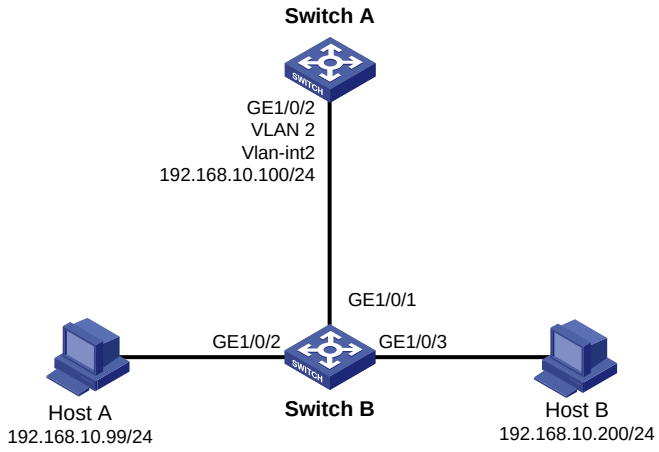
```
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
[Switch-Vlan-interface2] proxy-arp enable
[Switch-Vlan-interface2] quit
```

## Local Proxy ARP Configuration Example in Case of Port Isolation

### Network requirements

- Host A and Host B belong to the same VLAN, and connect to Switch B via GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3, respectively.
- Switch B connects to Switch A via GigabitEthernet 1/0/1.
- On Switch B, Layer 2 and Layer 3 port isolation are configured on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. Enable proxy ARP on Switch A to allow communication between Host A and Host B.

**Figure 2-4** Network diagram for local proxy ARP between isolated ports




### Configuration procedure

1) Configure Switch B

# Add GigabitEthernet 1/0/3, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to VLAN 2. Host A and Host B are isolated and unable to exchange Layer 2 packets.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port-isolate enable
[SwitchB-GigabitEthernet1/0/3] quit
```

2) Configure Switch A

# Configure an IP address of VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.10.100 255.255.0.0
```

The ping operation from Host A to Host B is unsuccessful because they are isolated at Layer 2.

# Configure local proxy ARP to let Host A and Host B communicate at Layer 3.

```
[SwitchA-Vlan-interface2] local-proxy-arp enable
[SwitchA-Vlan-interface2] quit
```

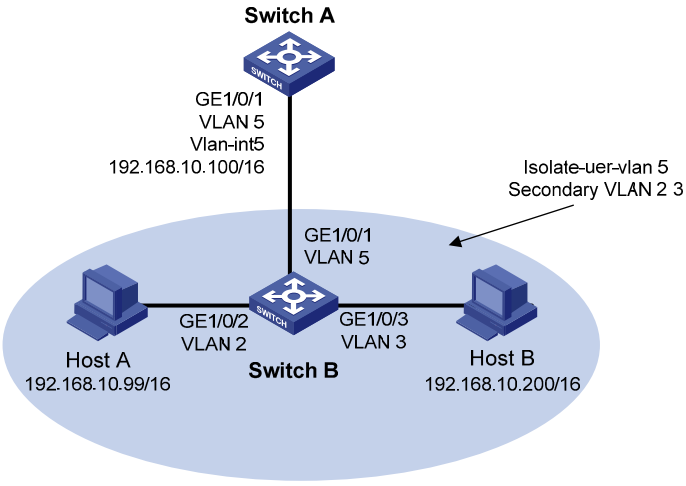
The ping operation from Host A to Host B is successful after the configuration.

## Local Proxy ARP Configuration Example in Isolate-user-vlan

### Network requirements

- Switch A is attached to Switch B through GigabitEthernet 1/0/1.
- VLAN 5 on Switch B is an isolate-user-vlan, which includes uplink port GigabitEthernet 1/0/1 and two secondary VLANs (VLAN 2 and VLAN 3). GigabitEthernet 1/0/2 belongs to VLAN 2, and GigabitEthernet 1/0/3 belongs to VLAN 3.
- Configure local proxy ARP on Switch A to implement Layer 3 communication between VLAN 2 and VLAN 3.

**Figure 2-5** Network diagram for local proxy ARP configuration in isolate-user-vlan




### Configuration procedure

1) Configure Switch B

# Create VLAN 2, VLAN 3, and VLAN 5 on Switch B. Add GigabitEthernet 1/0/2 to VLAN 2, GigabitEthernet 1/0/3 to VLAN 3, and GigabitEthernet 1/0/1 to VLAN 5. Configure VLAN 5 as the isolate-user-vlan, and VLAN 2 and VLAN 3 as secondary VLANs. Configure the mappings between isolate-user-vlan and the secondary VLANs.

```
<SwitchB> system-view
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/1
[SwitchB-vlan5] isolate-user-vlan enable
[SwitchB-vlan5] quit
[SwitchB] isolate-user-vlan 5 secondary 2 3
```

2) Configure Switch A

# Create VLAN 5 and add GigabitEthernet 1/0/1 to it.

```
<SwitchA> system-view
[SwitchA] vlan 5
[SwitchA-vlan5] port gigabitethernet 1/0/1
[SwitchA-vlan5] interface vlan-interface 5
[SwitchA-Vlan-interface5] ip address 192.168.10.100 255.255.0.0
```

The ping operation from Host A to Host B is unsuccessful because they are isolated at Layer 2.

# Configure local proxy ARP to implement communication between VLAN 2 and VLAN 3.

```
[SwitchA-Vlan-interface5] local-proxy-arp enable
[SwitchA-Vlan-interface5] quit
```

The ping operation from Host A to Host B is successful after the configuration.

# 3 ARP Attack Defense Configuration

When configuring ARP attack defense, go to these sections for information you are interested in:



Although ARP is easy to implement, it provides no security mechanism and thus is prone to network attacks. Currently, ARP attacks and viruses are threatening LAN security. The device can provide multiple features to detect and prevent such attacks. This chapter mainly introduces these features.

## Configuring ARP Source Suppression

### Introduction to ARP Source Suppression

If a device receives large numbers of IP packets from a host to unreachable destinations,

- The device sends large numbers of ARP requests to the destination subnets, which increases the load of the destination subnets.
- The device continuously resolves destination IP addresses, which increases the load of the CPU.

To protect the device from such attacks, you can enable the ARP source suppression function. With the function enabled, whenever the number of packets with unresolvable destination IP addresses from a host within five seconds exceeds a specified threshold, the device suppresses the sending host from triggering any ARP requests within the following five seconds.

### Configuring ARP Source Suppression

Follow these steps to configure ARP source suppression:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable ARP source suppression | **arp source-suppression enable** | Required<br>Disabled by default. |
| Set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five consecutive seconds | **arp source-suppression limit** *limit-value* | Optional<br>10 by default. |

### Displaying and Maintaining ARP Source Suppression

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the ARP source suppression configuration information | **display arp source-suppression** | Available in any view |

# Configuring ARP Defense Against IP Packet Attacks

## Introduction to ARP Defense Against IP Packet Attacks

When forwarding an IP packet, a device depends on ARP to resolve the MAC address of the next hop. If the address resolution is successful, the forwarding chip forwards the packet directly. Otherwise, the device runs software for further processing. If the device cannot resolve the next hops for large numbers of incoming packets, the CPU of the device will be exhausted. This is called IP packet attacks.

To protect a device against IP packet attacks, you can enable the ARP defense against IP packet attacks function. After receiving an IP packet whose next hop cannot be resolved by ARP, a device with this function enabled creates a black hole route immediately and the forwarding chip simply drops all packets matching the next hop during the age time of the black hole route.

## Enabling ARP Defense Against IP Packet Attacks

The ARP defense against IP packet attack function applies to packets to be forwarded and those originated by the device.

Follow these steps to configure ARP defense against IP packet attacks:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable ARP defense against IP packet attacks | **arp resolving-route enable** | Optional<br>Enabled by default. |

# Configuring ARP Active Acknowledgement

## Introduction

Typically, the ARP active acknowledgement feature is configured on gateway devices to identify invalid ARP packets.

With this feature enabled, the gateway, upon receiving an ARP packet with a different source MAC address from that in the corresponding ARP entry, checks whether the ARP entry has been updated within the last minute:

- If yes, the gateway does not update the ARP entry;
- If not, the gateway unicasts an ARP request to the source MAC address of the ARP entry.

Then,

- If an ARP reply is received within five seconds, the ARP packet is ignored;
- If not, the gateway unicasts an ARP request to the MAC address of the ARP packet.

Then,

- If an ARP reply is received within five seconds, the gateway updates the ARP entry;
- If not, the ARP entry is not updated.

### Configuring the ARP Active Acknowledgement Function

Follow these steps to configure ARP active acknowledgement:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the ARP active acknowledgement function | **arp anti-attack active-ack enable** | Required<br>Disabled by default. |

# Configuring Source MAC Address Based ARP Attack Detection

## Introduction

This feature allows the device to check the source MAC address of ARP packets. If the number of ARP packets sent from a MAC address within five seconds exceeds the specified value, the device considers this an attack.

Only the ARP packets delivered to the CPU are detected.

## Configuration Procedure

### Enabling source MAC address based ARP attack detection

After this feature is enabled for a device, if the number of ARP packets it receives from a MAC address within five seconds exceeds the specified value, it generates an alarm and filters out ARP packets sourced from that MAC address (in **filter** mode), or only generates an alarm (in **monitor** mode).

Follow these steps to configure source MAC address based ARP attack detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable source MAC address based ARP attack detection and specify the detection mode | **arp anti-attack source-mac** { **filter** \| **monitor** } | Required<br>Disabled by default. |

### Configuring protected MAC addresses

A protected MAC address is excluded from ARP attack detection even though it is an attacker. You can specify certain MAC addresses, such as that of a gateway or important servers, as protected MAC addresses.

Follow these steps to configure protected MAC addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure protected MAC addresses | **arp anti-attack source-mac exclude-mac** *mac-address*&<1-n> | Optional<br>Not configured by default. |

### Configuring the aging timer for protected MAC addresses

Follow these steps to configure the aging timer for protected MAC addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure aging timer for protected MAC addresses | **arp anti-attack source-mac aging-time** *time* | Optional<br>Five minutes by default. |

### Configuring the threshold

Follow these steps to configure the threshold:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the threshold | **arp anti-attack source-mac threshold** *threshold-value* | Optional<br>50 by default. |

## Displaying and Maintaining Source MAC Address Based ARP Attack Detection

| To do… | Use the command… | Remarks |
|---|---|---|
| Display attacking entries detected | **display arp anti-attack source-mac** [ **interface** *interface-type interface-number* ] | Available in any view |

**Note**

A protected MAC address is no longer excluded from detection after the specified aging time expires.

# Configuring ARP Packet Source MAC Address Consistency Check

## Introduction

This feature enables a gateway device to filter out ARP packets with the source MAC address in the Ethernet header different from the sender MAC address in the ARP message, so that the gateway device can learn correct ARP entries.

ARP detection also checks source MAC address consistency of ARP packets, but it is enabled on an access device to detect only ARP packets sent to it.

### Configuring ARP Packet Source MAC Address Consistency Check

Follow these steps to enable ARP packet source MAC address consistency check:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable ARP packet source MAC address consistency check | **arp anti-attack valid-check enable** | Required<br>Disabled by default. |

## Configuring ARP Packet Rate Limit

### Introduction

This feature allows you to limit the rate of ARP packets to be delivered to the CPU.

### Configuring the ARP Packet Rate Limit Function

Follow these steps to configure ARP packet rate limit:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure ARP packet rate limit | **arp rate-limit** { **disable \| rate** *pps* **drop** } | Required<br>By default, the ARP packet rate limit is enabled and is 100 pps. |

## Configuring ARP Detection

**Note**

- For information about DHCP snooping, refer to *DHCP Configuration* in the *IP Services Volume*.
- For information about 802.1X, refer to *802.1X Configuration* in the *Security Volume*.

### Introduction to ARP Detection

The ARP detection feature allows only the ARP packets of legal clients to be forwarded.

## Enabling ARP Detection Based on DHCP Snooping Entries/802.1x Security Entries/Static IP-to-MAC Bindings

With this feature enabled, the device compares the source IP and MAC addresses of an ARP packet received from the VLAN against the DHCP snooping entries, 802.1X security entries, or static IP-to-MAC binding entries. You can specify a detection type or types as needed. If all the detection types are specified, the system uses DHCP snooping entries first, then 802.1X security entries, and then IP-to-MAC bindings.

1) After you enable ARP detection based on DHCP snooping entries for a VLAN,

- Upon receiving an ARP packet from an ARP untrusted port, the device compares the ARP packet against the DHCP snooping entries. If a match is found, that is, the parameters (such as IP address, MAC addresses, port index, and VLAN ID) are consistent, the ARP packet passes the check; if not, the ARP packet cannot pass the check.
- Upon receiving an ARP packet from an ARP trusted port, the device does not check the ARP packet.
- If ARP detection is not enabled for the VLAN, the ARP packet is not checked even if it is received from an ARP untrusted port.

---

**Note**

ARP detection based on DHCP snooping entries involves both dynamic DHCP snooping entries and static IP Source Guard binding entries. Dynamic DHCP snooping entries are automatically generated through the DHCP snooping function. For details, refer to *DHCP Configuration* in the *IP Service Volume*. Static IP Source Guard binding entries are created by using the **user-bind** command. For details, refer to *IP Source Guard Configuration* in the *Security Volume*.

---

2) After you enable ARP detection based on 802.1X security entries, the device, upon receiving an ARP packet from an ARP untrusted port, compares the ARP packet against the 802.1X security entries.

- If an entry with matching source IP and MAC addresses, port index, and VLAN ID is found, the ARP packet is considered valid.
- If an entry with no matching IP address but with a matching OUI MAC address is found, the ARP packet is considered valid.

Otherwise, the packet is considered invalid and discarded.

3) After you enable ARP detection based on static IP-to-MAC bindings, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings.

- If an entry with a matching IP address but a different MAC address is found, the ARP packet is considered invalid and discarded.
- If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.
- If no match is found, the ARP packet is considered valid and can pass the detection.

Follow these steps to enable ARP detection for a VLAN and specify a trusted port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable ARP detection for the VLAN | **arp detection enable** | Required<br>Disabled by default. That is, the ARP packets received on all the ports in the VLAN will not be checked. |
| Return to system view | **quit** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Configure the port as a trusted port | **arp detection trust** | Optional<br>The port is an untrusted port by default. |
| Return to system view | **quit** | — |
| Specify an ARP attack detection mode | **arp detection mode** { **dhcp-snooping** \| **dot1x** \| **static-bind** } * | Required<br>No ARP attack detection mode is specified by default; that is, ARP detection based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings is not enabled by default. |
| Configure a static IP-to-MAC binding for ARP detection | **arp detection static-bind** *ip-address mac-address* | Optional<br>Not configured by default.<br>If the ARP attack detection mode is **static-bind**, you need to configure static IP-to-MAC bindings for ARP detection. |

**Caution**

During the DHCP assignment process, when the client receives the DHCP-ACK message from the DHCP server, it broadcasts a gratuitous ARP packet to detect address conflicts. If no response is received in a pre-defined time period, the client uses the assigned IP address. If the client is enabled with ARP detection based on 802.1X security entries, the IP address is not uploaded to the 802.1X device before the client uses the IP address. As a result, the gratuitous ARP packet is considered to be an attack packet and is discarded, and thus cannot detect conflicts. After the client uploads its IP address to the 802.1X device, subsequent ARP packets sent by the client are considered to be valid and are allowed to travel through.

## Configuring ARP Detection Based on Specified Objects

You can also specify objects in ARP packets to be detected. The objects involve:

- src-mac: Checks whether the sender MAC address of an ARP packet is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded; otherwise, the packet is discarded.
- dst-mac: Checks the target MAC address of ARP replies. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

- ip: Checks both the source and destination IP addresses in an ARP packet. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this object specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests are checked.

Before performing the following configuration, make sure you have configured the **arp detection enable** command.

Follow these steps to configure ARP detection based on specified objects:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify objects for ARP detection | **arp detection validate** { **dst-mac** \| **ip** \| **src-mac** } * | Required<br>Not specified by default. |

**Note**

- If both the ARP detection based on specified objects and the ARP detection based on snooping entries/802.1X security entries/static IP-to-MAC bindings are enabled, the former one applies first, and then the latter applies.
- Before enabling ARP detection based on DHCP snooping entries, make sure that DHCP snooping is enabled.
- Before enabling ARP detection based on 802.1X security entries, make sure that 802.1X is enabled and the 802.1X clients are configured to upload IP addresses.

## Displaying and Maintaining ARP Detection

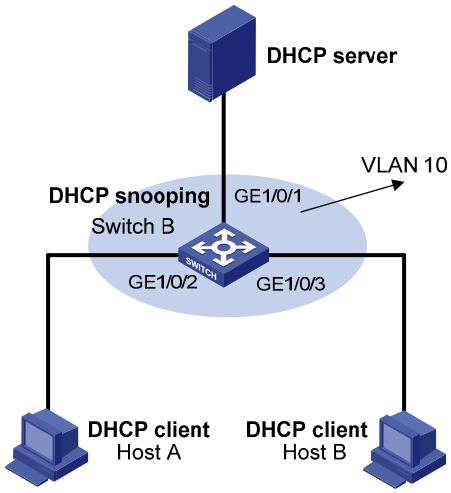
| To do… | Use the command… | Remarks |
|---|---|---|
| Display the VLANs enabled with ARP detection | **display arp detection** | Available in any view |
| Display the ARP detection statistics | **display arp detection statistics** [ **interface** *interface-type interface-number* ] | Available in any view |
| Clear the ARP detection statistics | **reset arp detection statistics** [ **interface** *interface-type interface-number* ] | Available in user view |

## ARP Detection Configuration Example I

### Network requirements

- Enable DHCP snooping on Switch B. Enable ARP detection for VLAN 10 to allow only packets from valid clients to pass.
- Configure Host A and Host B as DHCP clients.

**Figure 3-1** Network diagram for ARP detection configuration




## Configuration procedure

1) Add all the ports on Switch B into VLAN 10, and configure the IP address of VLAN-interface 10 on Switch A (the configuration procedure is omitted).
2) Configure a DHCP server (the configuration procedure is omitted).
3) Configure Host A and Host B as DHCP clients (the configuration procedure is omitted).
4) Configure Switch B

# Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# Enable ARP detection for VLAN 10. Configure the upstream port as a trusted port and the downstream ports as untrusted ports (a port is an untrusted port by default).

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
[SwitchB-vlan10] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp detection trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# Configure a static IP Source Guard binding entry on GigabitEthernet 1/0/2.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] user-bind ip-address 10.1.1.5 mac-address 0001-0203-0405
vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
```

# Configure a static IP Source Guard binding entry on GigabitEthernet 1/0/3.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] user-bind ip-address 10.1.1.6 mac-address 0001-0203-0607
vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
```

# Enable ARP detection based on both DHCP snooping entries and static IP-to-MAC bindings.

```
[SwitchB] arp detection mode dhcp-snooping static-bind
[SwitchB] arp detection static-bind 10.1.1.1 000f-e249-8050
```

# Enable the checking of the MAC addresses and IP addresses of ARP packets.

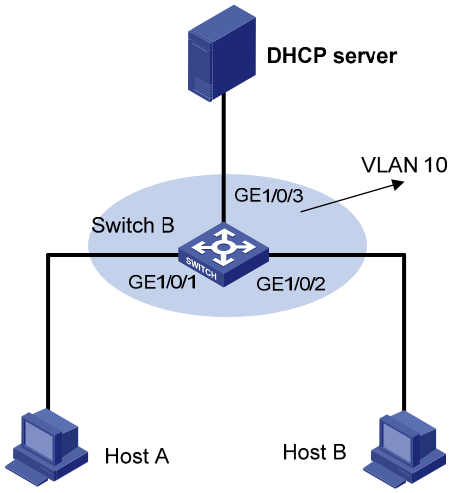
```
[SwitchB] arp detection validate dst-mac ip src-mac
```

## ARP Detection Configuration Example II

### Network requirements

- Enable 802.1X on Switch B. Enable ARP detection for VLAN 10 to allow only packets from valid clients to pass.
- Configure Host A and Host B as local 802.1X access users.

**Figure 3-2** Network diagram for ARP detection configuration




### Configuration procedure

1) Add all the ports on Switch B into VLAN 10, and configure the IP address of VLAN-interface 10 on Switch A (the configuration procedure is omitted).
2) Configure a DHCP server (the configuration procedure is omitted).
3) Configure Host A and Host B as 802.1x clients (the configuration procedure is omitted) and configure them to upload IP addresses for ARP detection.
4) Configure Switch B

# Enable the 802.1x function.

```
<SwitchB> system-view
[SwitchB] dot1x
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dot1x
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dot1x
[SwitchB-GigabitEthernet1/0/2] quit
```

# Add local access user **test**.

```
[SwitchB] local-user test
[SwitchB-luser-test] service-type lan-access
[SwitchB-luser-test] password simple test
```

```
[SwitchB-luser-test] quit
```

# Enable ARP detection for VLAN 10. Configure the upstream port as a trusted port and the downstream ports as untrusted ports (a port is an untrusted port by default).

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
[SwitchB-vlan10] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] arp detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

# Enable ARP detection based on 802.1X security entries.

```
[SwitchB] arp detection mode dot1x
```

# Table of Contents

This document is organized as follows:



# 1 DHCP Overview

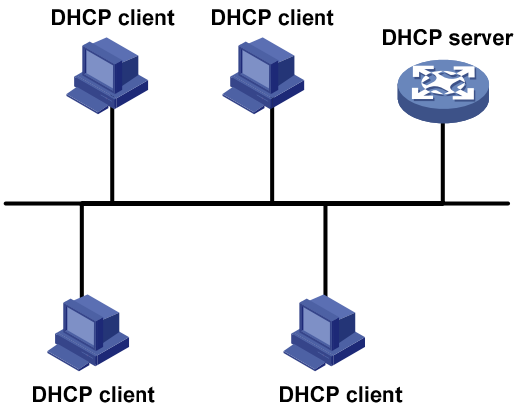
## Introduction to DHCP

The fast expansion and growing complexity of networks result in scarce IP addresses assignable to hosts. Meanwhile, as many people need to take their laptops across networks, the IP addresses need to be changed accordingly. Therefore, related configurations on hosts become more complex. The Dynamic Host Configuration Protocol (DHCP) was introduced to solve these problems.

DHCP is built on a client-server model, in which a client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client.

A typical DHCP application, as shown in Figure 1-1, includes a DHCP server and multiple clients (PCs and laptops).

**Figure 1-1** A typical DHCP application




**Note**

A DHCP client can get an IP address and other configuration parameters from a DHCP server on another subnet via a DHCP relay agent. For information about the DHCP relay agent, refer to Introduction to DHCP Relay Agent.

# DHCP Address Allocation

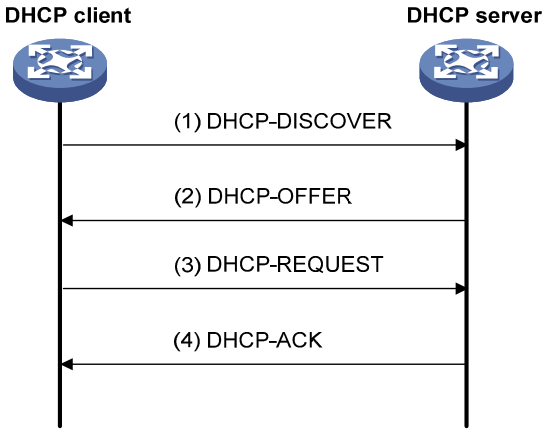
## Allocation Mechanisms

DHCP supports three mechanisms for IP address allocation.

- Manual allocation: The network administrator assigns an IP address to a client like a WWW server, and DHCP conveys the assigned address to the client.
- Automatic allocation: DHCP assigns a permanent IP address to a client.
- Dynamic allocation: DHCP assigns an IP address to a client for a limited period of time, which is called a lease. Most DHCP clients obtain their addresses in this way.

## Dynamic IP Address Allocation Process

**Figure 1-2** Dynamic IP address allocation process




As shown in Figure 1-2, a DHCP client obtains an IP address from a DHCP server via four steps:

1) The client broadcasts a DHCP-DISCOVER message to locate a DHCP server.
2) A DHCP server offers configuration parameters including an IP address to the client in a DHCP-OFFER message. The sending mode of the DHCP-OFFER message is determined by the flag field in the DHCP-DISCOVER message. Refer to DHCP Message Format for related information.
3) If several DHCP servers send offers to the client, the client accepts the first received offer, and broadcasts it in a DHCP-REQUEST message to formally request the IP address.
4) All DHCP servers receive the DHCP-REQUEST message, but only the server from which the client accepts the offered IP address responds. The server returns a DHCP-ACK message to the client, confirming that the IP address has been allocated to the client, or a DHCP-NAK unicast message, denying the IP address allocation.

**Note**

- After receiving the DHCP-ACK message, the client probes whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within a specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.
- The IP addresses offered by other DHCP servers are still assignable to other clients.

### IP Address Lease Extension

The IP address dynamically allocated by a DHCP server to a client has a lease. When the lease expires, the IP address is reclaimed by the DHCP server. If the client wants to use the IP address longer, it has to extend the lease duration.

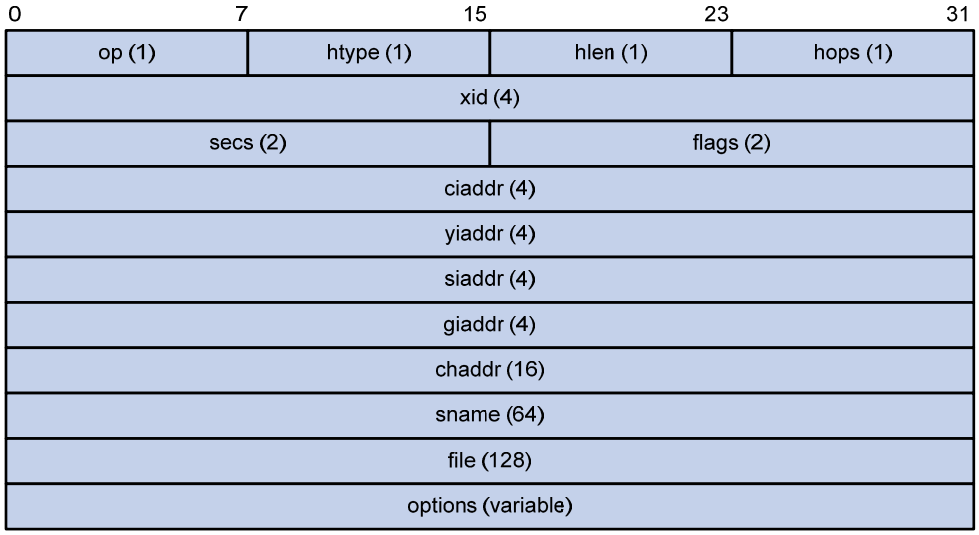
When the half lease duration elapses, the DHCP client sends to the DHCP server a DHCP-REQUEST unicast to extend the lease duration. Upon availability of the IP address, the DHCP server returns a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

If the client receives no reply, it broadcasts another DHCP-REQUEST message for lease extension after 7/8 lease duration elapses. The DHCP server handles the request as above mentioned.

## DHCP Message Format

Figure 1-3 gives the DHCP message format, which is based on the BOOTP message format and involves eight types. These types of messages have the same format except that some fields have different values. The numbers in parentheses indicate the size of each field in bytes.

**Figure 1-3** DHCP message format




- op: Message type defined in option field. 1 = REQUEST, 2 = REPLY
- htype, hlen: Hardware address type and length of a DHCP client.
- hops: Number of relay agents a request message traveled.
- xid: Transaction ID, a random number chosen by the client to identify an IP address allocation.

- secs: Filled in by the client, the number of seconds elapsed since the client began address acquisition or renewal process. Currently this field is reserved and set to 0.
- flags: The leftmost bit is defined as the BROADCAST (B) flag. If this flag is set to 0, the DHCP server sent a reply back by unicast; if this flag is set to 1, the DHCP server sent a reply back by broadcast. The remaining bits of the flags field are reserved for future use.
- ciaddr: Client IP address.
- yiaddr: 'your' (client) IP address, assigned by the server.
- siaddr: Server IP address, from which the clients obtained configuration parameters.
- giaddr: IP address of the first relay agent a request message traveled.
- chaddr: Client hardware address.
- sname: Server host name, from which the client obtained configuration parameters.
- file: Bootfile name and path information, defined by the server to the client.
- options: Optional parameters field that is variable in length, which includes the message type, lease, domain name server IP address, and WINS IP address.

# DHCP Options

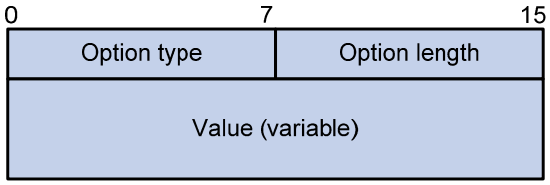
## DHCP Options Overview

The DHCP message adopts the same format as the Bootstrap Protocol (BOOTP) message for compatibility, but differs from it in the option field, which identifies new features for DHCP.

DHCP uses the option field in DHCP messages to carry control information and network configuration parameters, implementing dynamic address allocation and providing more network configuration information for clients.

Figure 1-4 shows the DHCP option format.

**Figure 1-4** DHCP option format




## Introduction to DHCP Options

The common DHCP options are as follows:

- Option 3: Router option. It specifies the gateway address to be assigned to the client.
- Option 6: DNS server option. It specifies the DNS server IP address to be assigned to the client.
- Option 51: IP address lease option.
- Option 53: DHCP message type option. It identifies the type of the DHCP message.
- Option 55: Parameter request list option. It is used by a DHCP client to request specified configuration parameters. The option contains values that correspond to the parameters requested by the client.
- Option 66: TFTP server name option. It specifies a TFTP server to be assigned to the client.
- Option 67: Bootfile name option. It specifies the bootfile name to be assigned to the client.
- Option 150: TFTP server IP address option. It specifies the TFTP server IP address to be assigned to the client.

- Option 121: Classless route option. It specifies a list of classless static routes (the destination addresses in these static routes are classless) that the requesting client should add to its routing table.
- Option 33: Static route option. It specifies a list of classful static routes (the destination addresses in these static routes are classful) that a client should add to its routing table. If Option 121 exists, Option 33 is ignored.

For more information about DHCP options, refer to RFC 2132.

## Self-Defined Options

Some options, such as Option 43, have no unified definitions in RFC 2132. The formats of some self-defined options are introduced as follows.

### Vendor-specific option (Option 43)

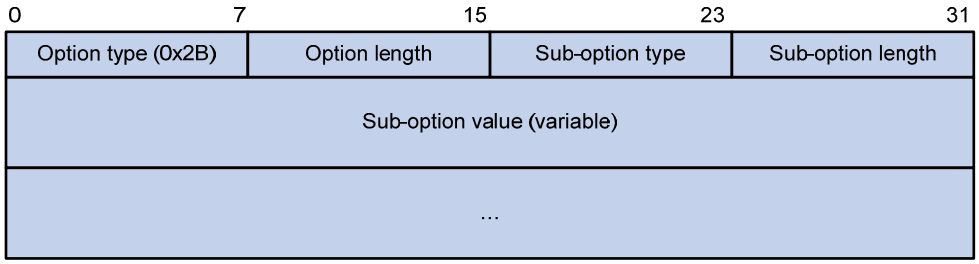
DHCP servers and clients exchange vendor-specific information through messages containing the vendor-specific option (Option 43). Upon receiving a DHCP message requesting Option 43 (in Option 55), the DHCP server returns a response message containing Option 43 to assign vendor-specific information to the DHCP client.

The DHCP client can obtain the following information through Option 43:

- Auto-Configuration Server (ACS) parameters, including the ACS URL, username, and password.
- Service provider identifier acquired by the customer premises equipment (CPE) from the DHCP server and sent to the ACS for selecting vender-specific configurations and parameters.
- Preboot Execution Environment (PXE) server address for further obtaining the bootfile or other control information from the PXE server.

1) Format of Option 43

**Figure 1-5** Format of Option 43



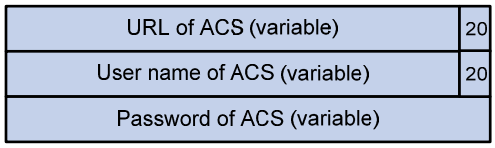

For the sake of scalability, network configuration parameters are carried in different sub-options of Option 43 so that the DHCP client can obtain more information through Option 43 as shown in Figure 1-5. The sub-option fields are described as follows:

- Sub-option type: Type of a sub-option. The field value can be 0x01, 0x02, or 0x80. 0x01 indicates an ACS parameter sub-option. 0x02 indicates a service provider identifier sub-option. 0x80 indicates a PXE server address sub-option.
- Sub-option length: Length of a sub-option excluding the sub-option type and sub-option length fields.
- Sub-option value: Value of a sub-option.

2) Format of the sub-option value field of Option 43

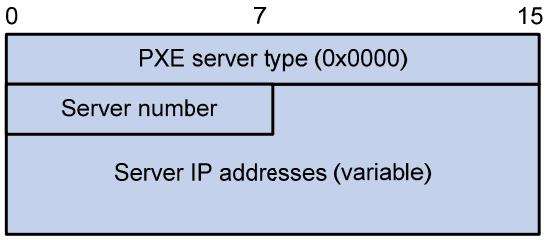
- As shown in Figure 1-6, the value field of the ACS parameter sub-option is filled in with variable ACS URL, username, and password separated with a space (0x20) in between.

**Figure 1-6** Format of the value field of the ACS parameter sub-option




- The value field of the service provider identifier sub-option contains the service provider identifier.
- Figure 1-7 shows the format of the value field of the PXE server address sub-option. Currently, the value of the PXE server type can only be 0. The server number field indicates the number of PXE servers contained in the sub-option. The server IP addresses filed contains the IP addresses of the PXE servers.

**Figure 1-7** Format of the value field of the PXE server address sub-option




## Relay agent option (Option 82)

Option 82 is the relay agent option in the option field of the DHCP message. It records the location information of the DHCP client. When a DHCP relay agent or DHCP snooping device receives a client's request, it adds Option 82 to the request message before forwarding the message to the server.

The administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. At least one sub-option is defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

Option 82 has no unified definition. Its padding formats vary with vendors.

You can use the following methods to configure Option 82:

- User-defined method: Manually specify the content of Option 82.
- Non-user-defined method: Pad Option 82 in the default normal or verbose format.

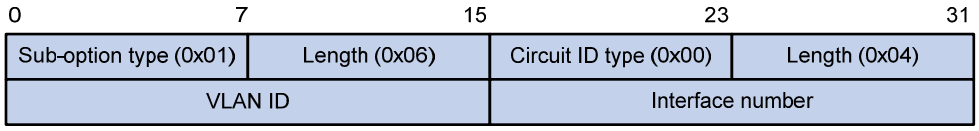
If you choose the second method, specify the code type for the sub-options as ASCII or HEX.

1) Normal padding format

The padding contents for sub-options in the normal padding format are as follows:

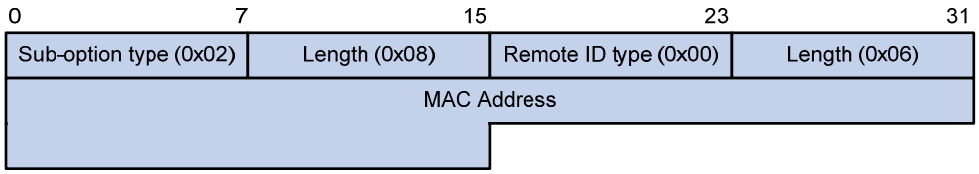
- Sub-option 1: Padded with the VLAN ID and interface number of the interface that received the client's request. The following figure gives its format. The value of the sub-option type is 1, and that of the circuit ID type is 0.

**Figure 1-8** Sub-option 1 in normal padding format




- Sub-option 2: Padded with the MAC address of the DHCP relay agent interface or the MAC address of the DHCP snooping device that received the client's request. The following figure gives its format. The value of the sub-option type is 2, and that of the remote ID type is 0.

**Figure 1-9** Sub-option 2 in normal padding format

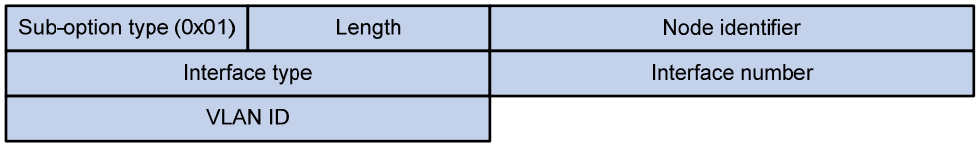



2) Verbose padding format

The padding contents for sub-options in the verbose padding format are as follows:

- Sub-option 1: Padded with the user-specified access node identifier (ID of the device that adds Option 82 in DHCP messages), and the type, number, and VLAN ID of the interface that received the client's request. Its format is shown in Figure 1-10.

**Figure 1-10** Sub-option 1 in verbose padding format




---

**Note**

In Figure 1-10, except that the VLAN ID field has a fixed length of 2 bytes, all the other padding contents of sub-option 1 are length variable.

---

- Sub-option 2: Padded with the MAC address of the DHCP relay agent interface or the MAC address of the DHCP snooping device that received the client's request. It has the same format as that in normal padding format, as shown in Figure 1-9.

## Option 184

Option 184 is a reserved option, and parameters in the option can be defined as needed. The device supports Option 184 carrying the voice related parameters, so a DHCP client with voice functions can get an IP address along with specified voice parameters from the DHCP server.

Option 184 involves the following sub-options:

- Sub-option 1: IP address of the primary network calling processor, which is a server serving as the network calling control source and providing program downloads.
- Sub-option 2: IP address of the backup network calling processor that DHCP clients will contact when the primary one is unreachable.
- Sub-option 3: Voice VLAN ID and the result whether DHCP clients take this ID as the voice VLAN or not.
- Sub-option 4: Failover route that specifies the destination IP address and the called number (SIP users use such IP addresses and numbers to communicate with each other) that a SIP user uses to reach another SIP user when both the primary and backup calling processors are unreachable.

---

**Note**

You must define the sub-option 1 to make other sub-options effective.

---

## Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 3046: DHCP Relay Agent Information Option

# 2 DHCP Relay Agent Configuration

When configuring the DHCP relay agent, go to these sections for information you are interested in:



**Note**

- The DHCP relay agent configuration is supported only on VLAN interfaces.
- DHCP snooping must be disabled on the DHCP relay agent.

## Introduction to DHCP Relay Agent

### Application Environment

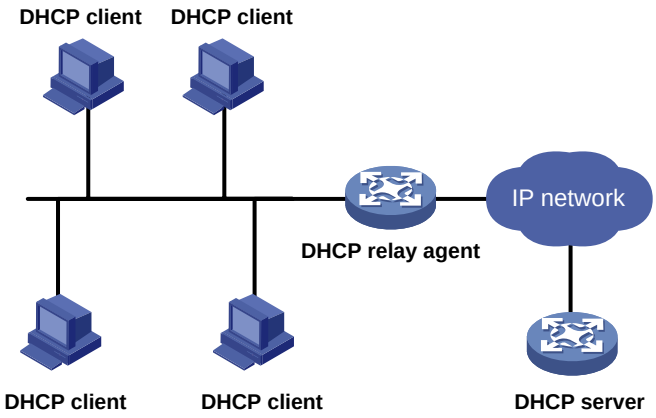
Since DHCP clients request IP addresses via broadcast messages, the DHCP server and clients must be on the same subnet. Therefore, a DHCP server must be available on each subnet, which is not practical.

DHCP relay agent solves the problem. Via a relay agent, DHCP clients communicate with a DHCP server on another subnet to obtain configuration parameters. Thus, DHCP clients on different subnets can contact the same DHCP server for ease of centralized management and cost reduction.

### Fundamentals

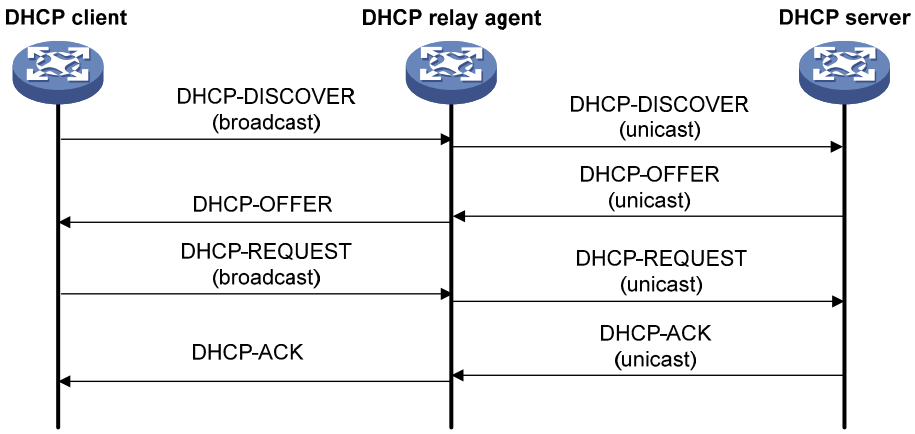
Figure 2-1 shows a typical application of the DHCP relay agent.

**Figure 2-1** DHCP relay agent application




No matter whether a relay agent exists or not, the DHCP server and client interact with each other in a similar way (see section Dynamic IP Address Allocation Process). The following describes the forwarding process on the DHCP relay agent.

**Figure 2-2** DHCP relay agent work process




As shown in Figure 2-2, the DHCP relay agent works as follows:

1) After receiving a DHCP-DISCOVER or DHCP-REQUEST broadcast message from a DHCP client, the DHCP relay agent fills the giaddr field of the message with its IP address and forwards the message to the designated DHCP server in unicast mode.
2) Based on the giaddr field, the DHCP server returns an IP address and other configuration parameters to the relay agent, which conveys them to the client.

## DHCP Relay Agent Support for Option 82

Option 82 records the location information of the DHCP client. The administrator can locate the DHCP client to further implement security control and accounting. For more information, refer toRelay agent option (Option 82).

If the DHCP relay agent supports Option 82, it will handle a client's request according to the contents defined in Option 82, if any. The handling strategies are described in the table below.

If a reply returned by the DHCP server contains Option 82, the DHCP relay agent will remove the Option 82 before forwarding the reply to the client.

| If a client's requesting message has… | Handling strategy | Padding format | The DHCP relay agent will… |
|---|---|---|---|
| Option 82 | Drop | Random | Drop the message. |
| | Keep | Random | Forward the message without changing Option 82. |
| | Replace | normal | Forward the message after replacing the original Option 82 with the Option 82 padded in normal format. |
| | | verbose | Forward the message after replacing the original Option 82 with the Option 82 padded in verbose format. |
| | | user-defined | Forward the message after replacing the original Option 82 with the user-defined Option 82. |
| no Option 82 | — | normal | Forward the message after adding the Option 82 padded in normal format. |
| | — | verbose | Forward the message after adding the Option 82 padded in verbose format. |
| | — | user-defined | Forward the message after adding the user-defined Option 82. |

# DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

| Task | Remarks |
|---|---|
| Enabling DHCP | Required |
| Enabling the DHCP Relay Agent on an Interface | Required |
| Correlating a DHCP Server Group with a Relay Agent Interface | Required |
| Configuring the DHCP Relay Agent Security Functions | Optional |
| Configuring the DHCP Relay Agent to Send a DHCP-Release Request | Optional |
| Configuring the DHCP Relay Agent to Support Option 82 | Optional |

# Configuring the DHCP Relay Agent

## Enabling DHCP

Enable DHCP before performing other DHCP-related configurations.

Follow these steps to enable DHCP:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable DHCP | **dhcp enable** | Required<br>Disabled by default. |

## Enabling the DHCP Relay Agent on an Interface

With this task completed, upon receiving a DHCP request from the enabled interface, the relay agent will forward the request to a DHCP server for address allocation.

Follow these steps to enable the DHCP relay agent on an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the DHCP relay agent on the current interface | **dhcp select relay** | Required<br>With DHCP enabled, interfaces work in the DHCP server mode. |

**Note**

If the DHCP client obtains an IP address via the DHCP relay agent, the address pool of the subnet to which the IP address of the DHCP relay agent belongs must be configured on the DHCP server. Otherwise, the DHCP client cannot obtain a correct IP address.

## Correlating a DHCP Server Group with a Relay Agent Interface

To improve reliability, you can specify several DHCP servers as a group on the DHCP relay agent and correlate a relay agent interface with the server group. When the interface receives requesting messages from clients, the relay agent will forward them to all the DHCP servers of the group.

Follow these steps to correlate a DHCP server group with a relay agent interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a DHCP server group and add a server into the group | **dhcp relay server-group** *group-id* **ip** *ip-address* | Required<br>Not created by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Correlate the DHCP server group with the current interface | **dhcp relay server-select** *group-id* | Required<br>By default, no interface is correlated with any DHCP server group. |

**Note**

- You can specify up to twenty DHCP server groups on the relay agent and eight DHCP server addresses for each DHCP server group.
- The IP addresses of DHCP servers and those of relay agent's interfaces cannot be on the same subnet. Otherwise, the client cannot obtain an IP address.
- A DHCP server group can correlate with one or multiple DHCP relay agent interfaces, while a relay agent interface can only correlate with one DHCP server group. Using the **dhcp relay server-select** command repeatedly overwrites the previous configuration. However, if the specified DHCP server group does not exist, the interface still uses the previous correlation.
- The *group-id* argument in the **dhcp relay server-select** command was specified by the **dhcp relay server-group** command.

## Configuring the DHCP Relay Agent Security Functions

### Creating static bindings and enable IP address check

The DHCP relay agent can dynamically record clients' IP-to-MAC bindings after clients get IP addresses. It also supports static bindings, which means you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses.

For avoidance of invalid IP address configuration, you can configure the DHCP relay agent to check whether a requesting client's IP and MAC addresses match a binding (both dynamic and static bindings) on the DHCP relay agent. If not, the client cannot access outside networks via the DHCP relay agent.

Follow these steps to create a static binding and enable IP address check:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a static binding | **dhcp relay security static** *ip-address mac-address* [ **interface** *interface-type interface-number* ] | Optional<br>No static binding is created by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable invalid IP address check | **dhcp relay address-check** { **disable** \| **enable** } | Required<br>Disabled by default. |

**Note**

- The **dhcp relay address-check enable** command is independent of other commands of the DHCP relay agent. That is, the invalid address check takes effect when this command is executed, regardless of whether other commands are used.
- The **dhcp relay address-check enable** command only checks IP and MAC addresses of clients.
- You are recommended to configure IP address check on the interface enabled with the DHCP relay agent; otherwise, the valid DHCP clients may not be capable of accessing networks.
- When using the **dhcp relay security static** command to bind an interface to a static binding entry, make sure that the interface is configured as a DHCP relay agent; otherwise, address entry conflicts may occur.

### Configuring dynamic binding update interval

Via the DHCP relay agent, a DHCP client sends a DHCP-RELEASE unicast message to the DHCP server to relinquish its IP address. In this case the DHCP relay agent simply conveys the message to the DHCP server, thus it does not remove the IP address from its bindings. To solve this problem, the DHCP relay agent can update dynamic bindings at a specified interval.

The DHCP relay agent uses the IP address of a client and the MAC address of the DHCP relay interface to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within a specified interval, which means the IP address is assignable now, the DHCP relay agent will update its bindings by aging out the binding entry of the IP address.
- If the server returns a DHCP-NAK message, which means the IP address is still in use, the relay agent will not age it out.

Follow these steps to configure dynamic binding update interval:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure binding update interval | **dhcp relay security tracker** { *interval* \| **auto** } | Optional<br>**auto** by default. (**auto** interval is calculated by the relay agent according to the number of bindings.) |

### Enabling unauthorized DHCP servers detection

There are unauthorized DHCP servers on networks, which reply DHCP clients with wrong IP addresses.

With this feature enabled, upon receiving a DHCP request, the DHCP relay agent will record the IP address of the DHCP server which assigned an IP address to the DHCP client and the receiving interface. The administrator can use this information to check out any DHCP unauthorized servers.

Follow these steps to enable unauthorized DHCP server detection:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable unauthorized DHCP server detection | **dhcp relay server-detect** | Required<br>Disabled by default. |

**Note**

With the unauthorized DHCP server detection enabled, the device puts a record once for each DHCP server. The administrator needs to find unauthorized DHCP servers from the log information. After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.

## Configuring the DHCP Relay Agent to Send a DHCP-Release Request

This task allows you to release a client's IP address manually on the DHCP relay agent. After you configure this task, the DHCP relay agent actively sends a DHCP-RELEASE request that contains the client's IP address to be released. Upon receiving the DHCP-RELEASE request, the DHCP server then releases the IP address for the client; meanwhile, the client's IP-to-MAC binding entry is removed from the DHCP relay agent.

Follow these steps to configure the DHCP relay agent in system view to send a DHCP-RELEASE request:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the DHCP relay agent to send a DHCP-RELEASE request | **dhcp relay release ip** *client-ip* | Required |

## Configuring the DHCP Relay Agent to Support Option 82

### Prerequisites

You need to complete the following tasks before configuring the DHCP relay agent to support Option 82.

- Enabling DHCP
- Enabling the DHCP relay agent on the specified interface
- Correlating a DHCP server group with relay agent interfaces

### Configuring the DHCP relay agent to support Option 82

Follow these steps to configure the DHCP relay agent to support Option 82:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view | | **interface** *interface-type interface-number* | — |
| Enable the relay agent to support Option 82 | | **dhcp relay information enable** | Required<br>Disabled by default. |
| Configure the handling strategy for requesting messages containing Option 82 | | **dhcp relay information strategy** { **drop** \| **keep** \| **replace** } | Optional<br>**replace** by default. |
| Configure non-user-defined Option 82 | Configure the padding format for Option 82 | **dhcp relay information format** { **normal** \| **verbose** [ **node-identifier** { **mac** \| **sysname** \| **user-defined** *node-identifier* } ] } | Optional<br>**normal** by default. |
| | Configure the code type for the circuit ID sub-option | **dhcp relay information circuit-id format-type** { **ascii** \| **hex** } | Optional<br>By default, the code type depends on the padding format of Option 82. Each field has its own code type.<br>The code type configuration applies to non-user-defined Option 82 only. |
| | Configure the code type for the remote ID sub-option | **dhcp relay information remote-id format-type** { **ascii** \| **hex** } | Optional<br>By default, the code type is **hex**.<br>This code type configuration applies to non-user-defined Option 82 only. |
| Configure user-defined Option 82 | Configure the padding content for the circuit ID sub-option | **dhcp relay information circuit-id string** *circuit-id* | Optional<br>By default, the padding content depends on the padding format of Option 82. |
| | Configure the padding content for the remote ID sub-option | **dhcp relay information remote-id string** { *remote-id* \| **sysname** } | Optional<br>By default, the padding content depends on the padding format of Option 82. |

**Note**

- To support Option 82, it is required to perform related configuration on both the DHCP server and relay agent.
- If the handling strategy of the DHCP relay agent is configured as **replace**, you need to configure a padding format for Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
- If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.

# Displaying and Maintaining DHCP Relay Agent Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about DHCP server groups correlated to a specified or all interfaces | **display dhcp relay** { **all** \| **interface** *interface-type interface-number* } | Available in any view |
| Display Option 82 configuration information on the DHCP relay agent | **display dhcp relay information** { **all** \| **interface** *interface-type interface-number* } | |
| Display information about bindings of DHCP relay agents | **display dhcp relay security** [ *ip-address* \| **dynamic** \| **static** ] | |
| Display statistics information about bindings of DHCP relay agents | **display dhcp relay security statistics** | |
| Display information about the refreshing interval for entries of dynamic IP-to-MAC bindings | **display dhcp relay security tracker** | |
| Display information about the configuration of a specified or all DHCP server groups | **display dhcp relay server-group** { *group-id* \| **all** } | |
| Display packet statistics on relay agent | **display dhcp relay statistics** [ **server-group** { *group-id* \| **all** } ] | |
| Clear packet statistics from relay agent | **reset dhcp relay statistics** [ **server-group** *group-id* ] | Available in user view |

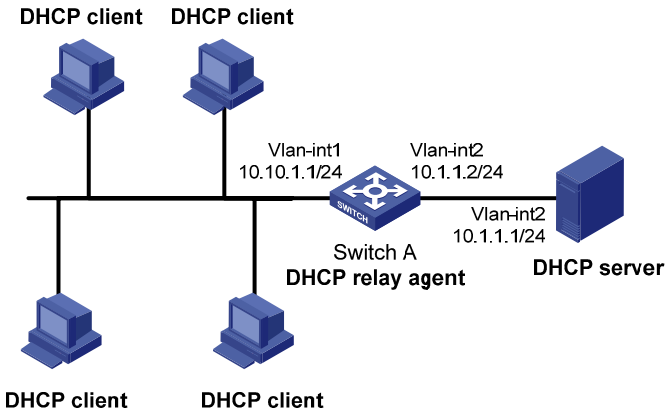
# DHCP Relay Agent Configuration Examples

## DHCP Relay Agent Configuration Example

### Network requirements

VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and IP address of VLAN-interface 2 is 10.1.1.2/24 that communicates with the DHCP server 10.1.1.1/24. As shown in Figure 2-3, Switch A forwards messages between DHCP clients and the DHCP server.

**Figure 2-3** Network diagram for DHCP relay agent



### Configuration procedure

# Specify IP addresses for the interfaces (omitted).

# Enable DHCP.

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

# Add DHCP server 10.1.1.1 into DHCP server group 1.

```
[SwitchA] dhcp relay server-group 1 ip 10.1.1.1
```

# Enable the DHCP relay agent on VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp select relay
```

# Correlate VLAN-interface 1 to DHCP server group 1.

```
[SwitchA-Vlan-interface1] dhcp relay server-select 1
```

---

**Note**

Because the DHCP relay agent and server are on different subnets, you need to configure a static route or dynamic routing protocol to make them reachable to each other.

---

## DHCP Relay Agent Option 82 Support Configuration Example

### Network requirements

- As shown in Figure 2-3, Enable Option 82 on the DHCP relay agent (Switch A).
- Configure the handling strategy for DHCP requests containing Option 82 as **replace**.
- Configure the padding content for the circuit ID sub-option as **company001** and for the remote ID sub-option as **device001**.
- Switch A forwards DHCP requests to the DHCP server after replacing Option 82 in the requests, so that the DHCP clients can obtain IP addresses.

### Configuration procedure

# Specify IP addresses for the interfaces (omitted).

# Enable DHCP.

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

# Add DHCP server 10.1.1.1 into DHCP server group 1.

```
[SwitchA] dhcp relay server-group 1 ip 10.1.1.1
```

# Enable the DHCP relay agent on VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp select relay
```

# Correlate VLAN-interface 1 to DHCP server group 1.

```
[SwitchA-Vlan-interface1] dhcp relay server-select 1
```

# Enable the DHCP relay agent to support Option 82, and perform Option 82-related configurations.

```
[SwitchA-Vlan-interface1] dhcp relay information enable
[SwitchA-Vlan-interface1] dhcp relay information strategy replace
[SwitchA-Vlan-interface1] dhcp relay information circuit-id string company001
[SwitchA-Vlan-interface1] dhcp relay information remote-id string device001
```

---

**Note**

You need to perform corresponding configurations on the DHCP server to make the Option 82 configurations function normally.

---

# Troubleshooting DHCP Relay Agent Configuration

## Symptom

DHCP clients cannot obtain any configuration parameters via the DHCP relay agent.

## Analysis

Some problems may occur with the DHCP relay agent or server configuration. Enable debugging and execute the **display** command on the DHCP relay agent to view the debugging information and interface state information for locating the problem.

## Solution

Check that:

- The address pool on the same subnet where DHCP clients reside is available on the DHCP server.
- The routes between the DHCP server and DHCP relay agent are reachable.
- The relay agent interface connected to DHCP clients is correlated with correct DHCP server group and IP addresses for the group members are correct.

# 3 DHCP Client Configuration

When configuring the DHCP client, go to these sections for information you are interested in:



**Note**

- The DHCP client configuration is supported only on VLAN interfaces.
- When multiple VLAN interfaces with the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be a Windows 2000 Server or Windows 2003 Server.
- You are not recommended to enable both the DHCP client and the DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.

## Introduction to DHCP Client

With the DHCP client enabled on an interface, the interface will use DHCP to obtain configuration parameters such as an IP address from the DHCP server.

## Enabling the DHCP Client on an Interface

Follow these steps to enable the DHCP client on an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the DHCP client on the interface | **ip address dhcp-alloc** [ **client-identifier mac** *interface-type interface-number* ] | Required<br>Disabled by default. |

**Note**

- An interface can be configured to acquire an IP address in multiple ways, but these ways are mutually exclusive. The latest configuration will overwrite the previous one.
- After the DHCP client is enabled on an interface, no secondary IP address is configurable for the interface.
- If the IP address assigned by the DHCP server shares a network segment with the IP addresses of other interfaces on the device, the DHCP client enabled interface will not request any IP address of the DHCP server, unless the conflicted IP address is manually deleted and the interface is made UP again by first executing the **shutdown** command and then the **undo shutdown** command or the DHCP client is enabled on the interface by executing the **undo ip address dhcp-alloc** and **ip address dhcp-alloc** commands in sequence.

# Displaying and Maintaining the DHCP Client

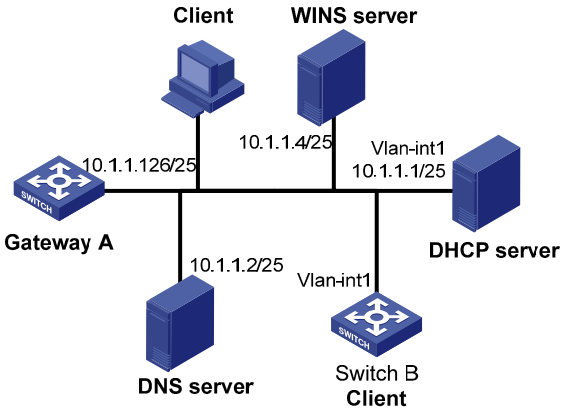
| To do… | Use the command… | Remarks |
|---|---|---|
| Display specified configuration information | **display dhcp client** [ **verbose** ] [ **interface** *interface-type interface-number* ] | Available in any view |

# DHCP Client Configuration Example

## Network requirements

As shown in Figure 3-1, on a LAN, Switch B contacts the DHCP server via VLAN-interface 1 to obtain an IP address.

**Figure 3-1** Network diagram for DHCP Client




## Configuration procedure

The following is the configuration on Switch B shown in Figure 3-1.

# Enable the DHCP client on VLAN-interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address dhcp-alloc
```

# 4 DHCP Snooping Configuration

When configuring DHCP snooping, go to these sections for information you are interested in:



**Note**

- The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.
- The DHCP snooping enabled device cannot be a DHCP relay agent.
- You are not recommended to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.

## DHCP Snooping Overview

### Function of DHCP Snooping

As a DHCP security feature, DHCP snooping can implement the following:

1) Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers
2) Recording IP-to-MAC mappings of DHCP clients

#### Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers

If there is an unauthorized DHCP server on a network, the DHCP clients may obtain invalid IP addresses and network configuration parameters, and cannot normally communicate with other network devices. With DHCP snooping, the ports of a device can be configured as trusted or untrusted, ensuring the clients to obtain IP addresses from authorized DHCP servers.

- Trusted: A trusted port forwards DHCP messages normally.
- Untrusted: An untrusted port discards the DHCP-ACK or DHCP-OFFER messages from any DHCP server.

You should configure ports that connecting to authorized DHCP servers and other DHCP snooping devices as trusted, and other ports as untrusted. With such configurations, DHCP clients obtain IP addresses from authorized DHCP servers only, while unauthorized DHCP servers cannot assign IP addresses to DHCP clients.

### Recording IP-to-MAC mappings of DHCP clients

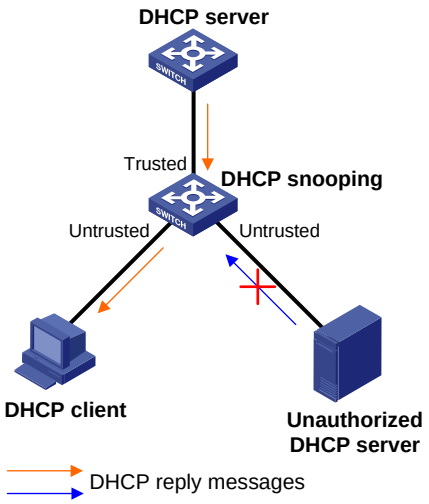
DHCP snooping reads DHCP-REQUEST messages and DHCP-ACK messages from trusted ports to record DHCP snooping entries, including MAC addresses of clients, IP addresses obtained by the clients, ports that connect to DHCP clients, and VLANs to which the ports belong. With DHCP snooping entries, DHCP snooping can implement the following:

- ARP detection: Whether ARP packets are sent from an authorized client is determined based on DHCP snooping entries. This feature prevents ARP attacks from unauthorized clients. For details, refer to *ARP Configuration* in the *IP Services Volume*.
- IP Source Guard: IP Source Guard uses dynamic binding entries generated by DHCP snooping to filter packets on a per-port basis, and thus prevents unauthorized packets from traveling through. For details, refer to *IP Source Guard Configuration* in the *Security Volume*.

## Application Environment of Trusted Ports

### Configuring a trusted port connected to a DHCP server

**Figure 4-1** Configure trusted and untrusted ports




As shown in Figure 4-1, a DHCP snooping device's port that is connected to an authorized DHCP server should be configured as a trusted port to forward reply messages from the DHCP server, so that the DHCP client is guaranteed to obtain IP addresses from the authorized DHCP server.

### Configuring trusted ports in a cascaded network

In a cascaded network involving multiple DHCP snooping devices, the ports connected to other DHCP snooping devices should be configured as trusted ports.

To save system resources, you can disable the trusted ports, which are indirectly connected to DHCP clients, from recording clients' IP-to-MAC bindings upon receiving DHCP requests.

**Figure 4-2** Configure trusted ports in a cascaded network

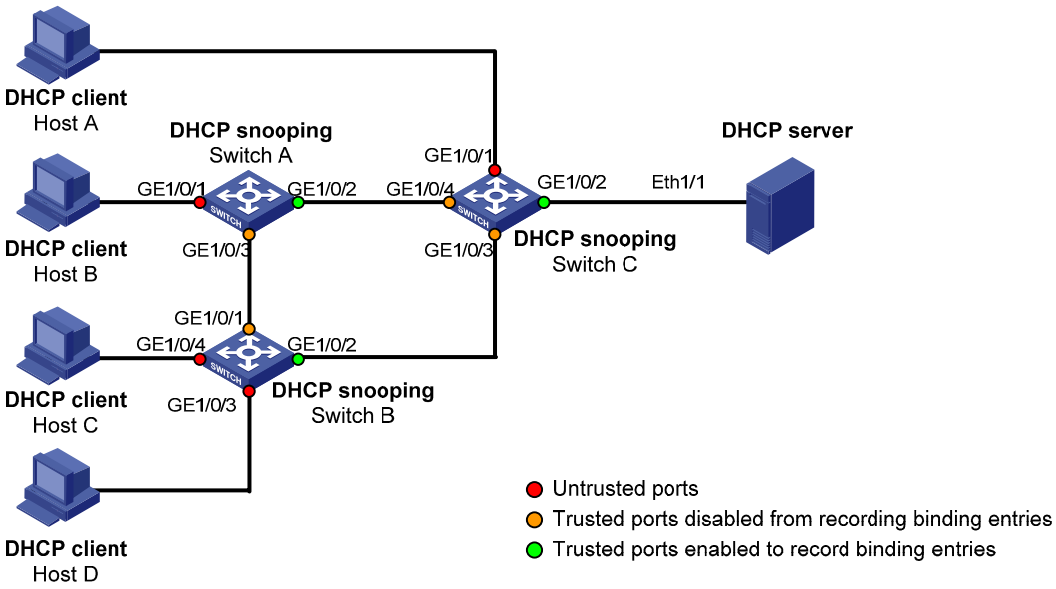



Table 4-1 describes roles of the ports shown in Figure 4-2.

**Table 4-1** Roles of ports

| Device | Untrusted port | Trusted port disabled from recording binding entries | Trusted port enabled to record binding entries |
|---|---|---|---|
| Switch A | GE1/0/1 | GE1/0/3 | GE1/0/2 |
| Switch B | GE1/0/3 and GE1/0/4 | GE1/0/1 | GE1/0/2 |
| Switch C | GE1/0/1 | GE1/0/3 and GE1/0/4 | GE1/0/2 |

## DHCP Snooping Support for Option 82

Option 82 records the location information of the DHCP client. The administrator can locate the DHCP client to further implement security control and accounting. For more information, refer to Relay agent option (Option 82).

If DHCP snooping supports Option 82, it will handle a client's request according to the contents defined in Option 82, if any. The handling strategies are described in the table below.

If a reply returned by the DHCP server contains Option 82, the DHCP snooping device will remove the Option 82 before forwarding the reply to the client. If the reply contains no Option 82, the DHCP snooping device forwards it directly.

| If a client's requesting message has… | Handling strategy | Padding format | The DHCP snooping device will… |
|---|---|---|---|
| Option 82 | Drop | Random | Drop the message. |
| | Keep | Random | Forward the message without changing Option 82. |
| | Replace | normal | Forward the message after replacing the original Option 82 with the Option 82 padded in normal format. |
| | | verbose | Forward the message after replacing the original Option 82 with the Option 82 padded in verbose format. |
| | | user-defined | Forward the message after replacing the original Option 82 with the user-defined Option 82. |
| no Option 82 | — | normal | Forward the message after adding the Option 82 padded in normal format. |
| | — | verbose | Forward the message after adding the Option 82 padded in verbose format. |
| | — | user-defined | Forward the message after adding the user-defined Option 82. |

**Note**

The handling strategy and padding format for Option 82 on the DHCP snooping device are the same as those on the relay agent.

## Configuring DHCP Snooping Basic Functions

Follow these steps to configure DHCP snooping basic functions:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable DHCP snooping | **dhcp-snooping** | Required<br>Disabled by default. |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Specify the port as trusted | **dhcp-snooping trust** [ **no-user-binding** ] | Required<br>Untrusted by default. |

**Note**

- You need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.
- You can specify Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces as trusted ports. For details about aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If a Layer 2 Ethernet interface is added to an aggregation group, DHCP snooping configured on the interface will not take effect. After the interface quits from the aggregation group, DHCP snooping will be effective.
- Do not add an untrusted Layer 2 Ethernet interface to an aggregation group.
- Configuring both the DHCP snooping and selective QinQ function on the switch is not recommended because it may result in malfunctioning of DHCP snooping.

# Configuring DHCP Snooping to Support Option 82

## Prerequisites

You need to enable the DHCP snooping function before configuring DHCP snooping to support Option 82.

## Configuring DHCP Snooping to Support Option 82

Follow these steps to configure DHCP snooping to support Option 82:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable DHCP snooping to support Option 82 | **dhcp-snooping information enable** | Required<br>Disabled by default. |
| Configure the handling strategy for requesting messages containing Option 82 | **dhcp-snooping information strategy** { **drop** \| **keep** \| **replace** } | Optional<br>**replace** by default. |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure non-user-defined Option 82 | Configure the padding format for Option 82 | **dhcp-snooping information format** { **normal** \| **verbose** [ **node-identifier** { **mac** \| **sysname** \| **user-defined** *node-identifier* } ] } | Optional<br>**normal** by default. |
| | Configure the code type for the circuit ID sub-option | **dhcp-snooping information circuit-id format-type** { **ascii** \| **hex** } | Optional<br>By default, the code type depends on the padding format of Option 82. Each field has its own code type.<br>This code type configuration applies to non-user-defined Option 82 only. |
| | Configure the code type for the remote ID sub-option | **dhcp-snooping information remote-id format-type** { **ascii** \| **hex** } | Optional<br>**hex** by default.<br>The code type configuration applies to non-user-defined Option 82 only. |
| Configure user-defined Option 82 | Configure the padding content for the circuit ID sub-option | **dhcp-snooping information** [ **vlan** *vlan-id* ] **circuit-id string** *circuit-id* | Optional<br>By default, the padding content depends on the padding format of Option 82. |
| | Configure the padding content for the remote ID sub-option | **dhcp-snooping information** [ **vlan** *vlan-id* ] **remote-id string** { *remote-id* \| **sysname** } | Optional<br>By default, the padding content depends on the padding format of Option 82. |

**Note**

- You can enable DHCP snooping to support Option 82 on Layer 2 Ethernet interfaces only.
- To support Option 82, it is required to perform related configuration on both the DHCP server and the device enabled with DHCP snooping.
- If the handling strategy of the DHCP-snooping-enabled device is configured as **replace**, you need to configure a padding format for Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
- If the Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP-snooping-enabled device will drop the message.

# Displaying and Maintaining DHCP Snooping

| To do… | Use the command… | Remarks |
|---|---|---|
| Display DHCP snooping entries | **display dhcp-snooping** [ **ip** *ip-address* ] | Available in any view |
| Display Option 82 configuration information on the DHCP snooping device | **display dhcp-snooping information** { **all** \| **interface** *interface-type interface-number* } | |
| Display DHCP packet statistics on the DHCP snooping device | **display dhcp-snooping packet statistics** | |
| Display information about trusted ports | **display dhcp-snooping trust** | |
| Clear DHCP snooping entries | **reset dhcp-snooping** { **all** \| **ip** *ip-address* } | Available in user view |
| Clear DHCP packet statistics on the DHCP snooping device | **reset dhcp-snooping packet statistics** | |

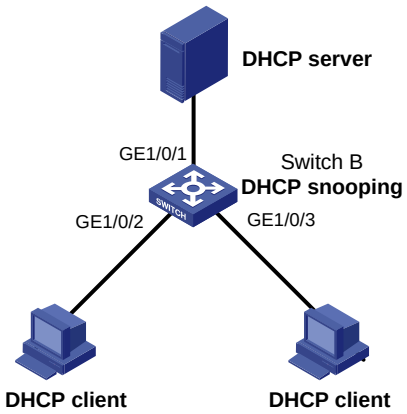
# DHCP Snooping Configuration Examples

## DHCP Snooping Configuration Example

### Network requirements

- As shown in Figure 4-3, Switch B is connected to a DHCP server through GigabitEthernet 1/0/1, and to two DHCP clients through GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
- GigabitEthernet 1/0/1 forwards DHCP server responses while the other two do not.
- Switch B records clients' IP-to-MAC address bindings in DHCP-REQUEST messages and DHCP-ACK messages received from trusted ports.

**Figure 4-3** Network diagram for DHCP snooping configuration




### Configuration procedure

# Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

# Specify GigabitEthernet 1/0/1 as trusted.

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

## DHCP Snooping Option 82 Support Configuration Example

### Network requirements

- As shown in Figure 4-3, enable DHCP snooping and Option 82 support on Switch B.
- Configure the handling strategy for DHCP requests containing Option 82 as **replace**.
- On GigabitEthernet 1/0/2, configure the padding content for the circuit ID sub-option as **company001** and for the remote ID sub-option as **device001**.
- On GigabitEthernet 1/0/3, configure the padding format as **verbose**, access node identifier as **sysname**, and code type as **ascii** for Option 82.
- Switch B forwards DHCP requests to the DHCP server after replacing Option 82 in the requests, so that the DHCP clients can obtain IP addresses.

### Configuration procedure

# Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

# Specify GigabitEthernet 1/0/1 as trusted.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 to support Option 82.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information enable
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information strategy replace
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information circuit-id string company001
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information remote-id string device001
[SwitchB-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 to support Option 82.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information enable
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information strategy replace
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information format verbose node-identifier
sysname
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information circuit-id format-type ascii
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information remote-id format-type ascii
```

# 5 BOOTP Client Configuration

While configuring a BOOTP client, go to these sections for information you are interested in:

- Introduction to BOOTP Client
- Configuring an Interface to Dynamically Obtain an IP Address Through BOOTP
- Displaying and Maintaining BOOTP Client Configuration

**Note**

- BOOTP client configuration only applies to VLAN interfaces.
- If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows 2000 Server or Windows 2003 Server.
- You are not recommended to enable both the DHCP client and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client may fail to obtain an IP address.

## Introduction to BOOTP Client

This section covers these topics:

- BOOTP Application
- Obtaining an IP Address Dynamically
- Protocols and Standards

### BOOTP Application

After you specify an interface of a device as a BOOTP client, the interface can use BOOTP to get information (such as IP address) from the BOOTP server, which simplifies your configuration.

Before using BOOTP, an administrator needs to configure a BOOTP parameter file for each BOOTP client on the BOOTP server. The parameter file contains information such as MAC address and IP address of a BOOTP client. When a BOOTP client originates a request to the BOOTP server, the BOOTP server will search for the BOOTP parameter file and return the corresponding configuration information.

Because you need to configure a parameter file for each client on the BOOTP server, BOOTP usually runs under a relatively stable environment. If the network changes frequently, DHCP is more suitable.

**Note**

Because a DHCP server can interact with a BOOTP client, you can use the DHCP server to configure an IP address for the BOOTP client, without any BOOTP server.

### Obtaining an IP Address Dynamically

**Note**

A DHCP server can take the place of the BOOTP server in the following dynamic IP address acquisition.

A BOOTP client dynamically obtains an IP address from a BOOTP server in the following steps:

1) The BOOTP client broadcasts a BOOTP request, which contains its own MAC address.
2) The BOOTP server receives the request and searches the configuration file for the corresponding IP address and other information according to the MAC address of the BOOTP client. The BOOTP server then returns a BOOTP response to the BOOTP client.
3) The BOOTP client obtains the IP address from the received response.

### Protocols and Standards

Some protocols and standards related to BOOTP include:

- RFC 951: Bootstrap Protocol (BOOTP)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol

## Configuring an Interface to Dynamically Obtain an IP Address Through BOOTP

Follow these steps to configure an interface to dynamically obtain an IP address:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure an interface to dynamically obtain IP address through BOOTP | **ip address bootp-alloc** | Required<br>By default, an interface does not use BOOTP to obtain an IP address. |

# Displaying and Maintaining BOOTP Client Configuration

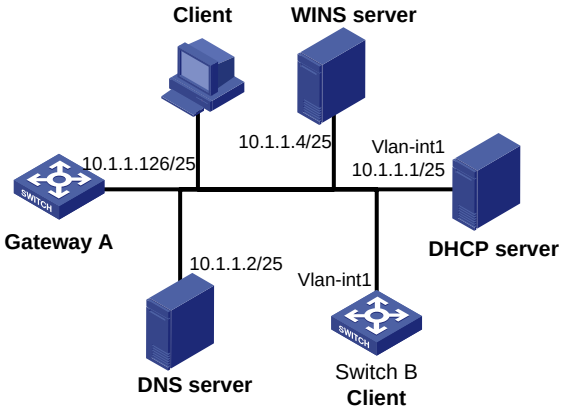
| To do… | Use the command… | Remarks |
|---|---|---|
| Display related information on a BOOTP client | **display bootp client** [ **interface** *interface-type interface-number* ] | Available in any view |

# BOOTP Client Configuration Example

## Network requirement

As shown in Figure 5-1, Switch B's port belonging to VLAN 1 is connected to the LAN. VLAN-interface 1 obtains an IP address from the DHCP server by using BOOTP.

**Figure 5-1** Network diagram for BOOTP




## Configuration procedure

The following describes only the configuration on Switch B serving as a client.

# Configure VLAN-interface 1 to dynamically obtain an IP address from the DHCP server.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address bootp-alloc
```

# Table of Contents

# 1 DNS Configuration

When configuring DNS, go to these sections for information you are interested in:



**Note**

This document only covers IPv4 DNS configuration. For information about IPv6 DNS configuration, refer to *IPv6 Basics Configuration* in the *IP Services Volume*.

## DNS Overview

Domain Name System (DNS) is a distributed database used by TCP/IP applications to translate domain names into corresponding IP addresses. With DNS, you can use easy-to-remember domain names in some applications and let the DNS server translate them into correct IP addresses.

There are two types of DNS services, static and dynamic. After a user specifies a name, the device checks the local static name resolution table for an IP address. If no IP address is available, it contacts the DNS server for dynamic name resolution, which takes more time than static name resolution. Therefore, some frequently queried name-to-IP address mappings are stored in the local static name resolution table to improve efficiency.

### Static Domain Name Resolution

The static domain name resolution means setting up mappings between domain names and IP addresses. IP addresses of the corresponding domain names can be found in the static domain resolution table when you use applications such as Telnet.

### Dynamic Domain Name Resolution

#### Resolving procedure

Dynamic domain name resolution is implemented by querying the DNS server. The resolution procedure is as follows:

1) A user program sends a name query to the resolver of the DNS client.
2) The DNS resolver looks up the local domain name cache for a match. If a match is found, it sends the corresponding IP address back. If not, it sends a query to the DNS server.

3) The DNS server looks up the corresponding IP address of the domain name in its DNS database. If no match is found, it sends a query to a higher level DNS server. This process continues until a result, whether successful or not, is returned.
4) The DNS client returns the resolution result to the application after receiving a response from the DNS server.

**Figure 1-1** Dynamic domain name resolution

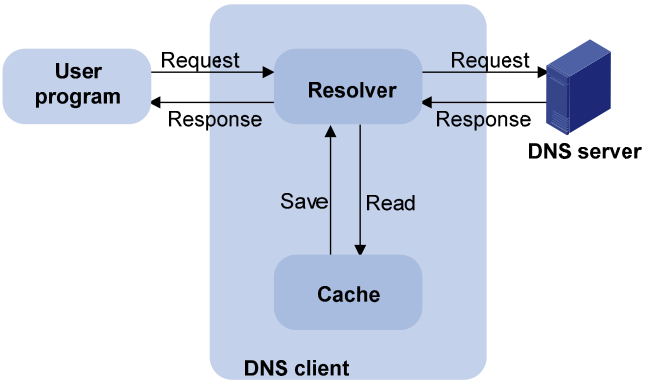



Figure 1-1 shows the relationship between the user program, DNS client, and DNS server.

The resolver and cache comprise the DNS client. The user program and DNS client can run on the same device or different devices, while the DNS server and the DNS client usually run on different devices.

Dynamic domain name resolution allows the DNS client to store latest mappings between domain names and IP addresses in the dynamic domain name cache. There is no need to send a request to the DNS server for a repeated query next time. The aged mappings are removed from the cache after some time, and latest entries are required from the DNS server. The DNS server decides how long a mapping is valid, and the DNS client gets the aging information from DNS messages.

## DNS suffixes

The DNS client normally holds a list of suffixes which can be defined by users. It is used when the name to be resolved is incomplete. The resolver can supply the missing part. For example, a user can configure com as the suffix for aabbcc.com. The user only needs to type aabbcc to get the IP address of aabbcc.com. The resolver can add the suffix and delimiter before passing the name to the DNS server.

- If there is no dot in the domain name (for example, aabbcc), the resolver will consider this a host name and add a DNS suffix before query. If no match is found after all the configured suffixes are used respectively, the original domain name (for example, aabbcc) is used for query.
- If there is a dot in the domain name (for example, www.aabbcc), the resolver will directly use this domain name for query. If the query fails, the resolver adds a DNS suffix for another query.
- If the dot is at the end of the domain name (for example, aabbcc.com.), the resolver will consider it a fully qualified domain name (FQDN) and return the query result, successful or failed. Hence, the dot "." at the end of the domain name is called the terminating symbol.

Currently, the device supports static and dynamic DNS services.

**Note**

If an alias is configured for a domain name on the DNS server, the device can resolve the alias into the IP address of the host.

# DNS Proxy

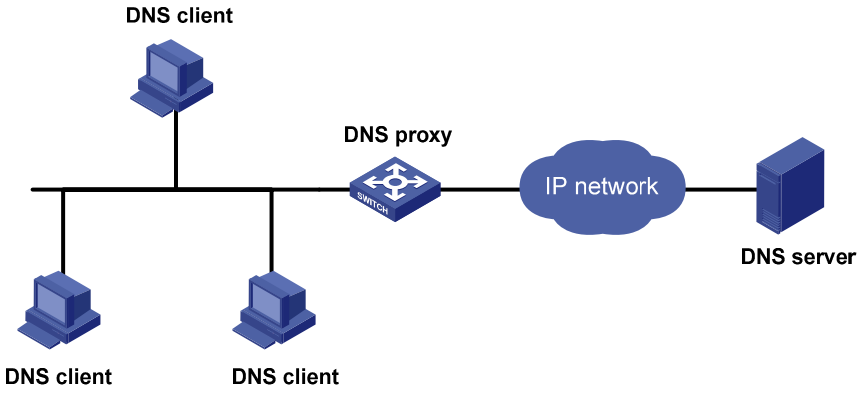
## Introduction to DNS proxy

A DNS proxy forwards DNS requests and replies between DNS clients and a DNS server.

As shown in Figure 1-2, a DNS client sends a DNS request to the DNS proxy, which forwards the request to the designated DNS server, and conveys the reply from the DNS server to the client.

The DNS proxy simplifies network management. When the DNS server address is changed, you only need to change the configuration on the DNS proxy instead of on each DNS client.

**Figure 1-2** DNS proxy networking application




## Operation of a DNS proxy

1) A DNS client considers the DNS proxy as the DNS server, and sends a DNS request to the DNS proxy, that is, the destination address of the request is the IP address of the DNS proxy.
2) The DNS proxy searches the local static domain name resolution table after receiving the request. If the requested information exists in the table, the DNS proxy returns a DNS reply to the client.
3) If the requested information does not exist in the static domain name resolution table, the DNS proxy sends the request to the designated DNS server for domain name resolution.
4) After receiving a reply from the DNS server, the DNS proxy forwards the reply to the DNS client.

# Configuring the DNS Client

## Configuring Static Domain Name Resolution

Follow these steps to configure static domain name resolution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a mapping between a host name and IP address in the static name resolution table | **ip host** *hostname ip-address* | Required<br>Not configured by default. |

**Note**

The IP address you last assign to the host name will overwrite the previous one if there is any.

You may create up to 50 static mappings between domain names and IP addresses.

## Configuring Dynamic Domain Name Resolution

Follow these steps to configure dynamic domain name resolution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable dynamic domain name resolution | **dns resolve** | Required<br>Disabled by default. |
| Specify a DNS server | **dns server** *ip-address* | Required<br>Not specified by default. |
| Configure a domain name suffix | **dns domain** *domain-name* | Optional<br>Not configured by default, that is, only the provided domain name is resolved. |

**Note**

You may configure up to six DNS servers and ten DNS suffixes.

# Configuring the DNS Proxy

Follow these steps to configure the DNS proxy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable DNS proxy | **dns proxy enable** | Required<br>Disabled by default. |

# Displaying and Maintaining DNS

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the static domain name resolution table | **display ip host** | Available in any view |
| Display DNS server information | **display dns server** [ **dynamic** ] | |
| Display domain name suffixes | **display dns domain** [ **dynamic** ] | Available in any view |
| Display the information of the dynamic domain name cache | **display dns dynamic-host** | |
| Clear the information of the dynamic domain name cache | **reset dns dynamic-host** | Available in user view |

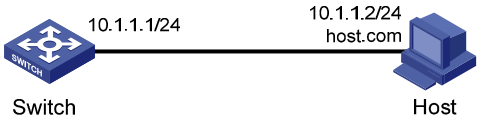
# DNS Configuration Examples

## Static Domain Name Resolution Configuration Example

### Network requirements

Switch uses the static domain name resolution to access Host with IP address 10.1.1.2 through domain name host.com.

**Figure 1-3** Network diagram for static domain name resolution




### Configuration procedure

# Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<Sysname> system-view
[Sysname] ip host host.com 10.1.1.2
```

# Execute the **ping host.com** command to verify that the Switch can use the static domain name resolution to get the IP address 10.1.1.2 corresponding to host.com.

```
[Sysname] ping host.com
  PING host.com (10.1.1.2):
```

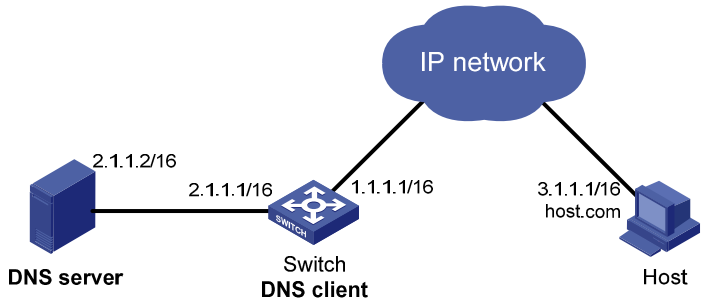
```
56  data bytes, press CTRL_C to break
  Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=128 time=1 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=128 time=4 ms
  Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=128 time=3 ms
  Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=128 time=2 ms
  Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=128 time=3 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/2/4 ms
```

## Dynamic Domain Name Resolution Configuration Example

### Network requirements

- The IP address of the DNS server is 2.1.1.2/16 and the name suffix is com. The mapping between domain name Host and IP address 3.1.1.1/16 is stored in the **com** domain.
- Switch serves as a DNS client, and uses the dynamic domain name resolution and the suffix to access the host with the domain name host.com and the IP address 3.1.1.1/16.

**Figure 1-4** Network diagram for dynamic domain name resolution




### Configuration procedure

---

**Note**

- Before performing the following configuration, make sure that there is a route between the Switch and the host, and the IP addresses of the interfaces are configured as shown Figure 1-4.
- This configuration may vary with different DNS servers. The following configuration is performed on a Windows server 2000.

---

1) Configure the DNS server

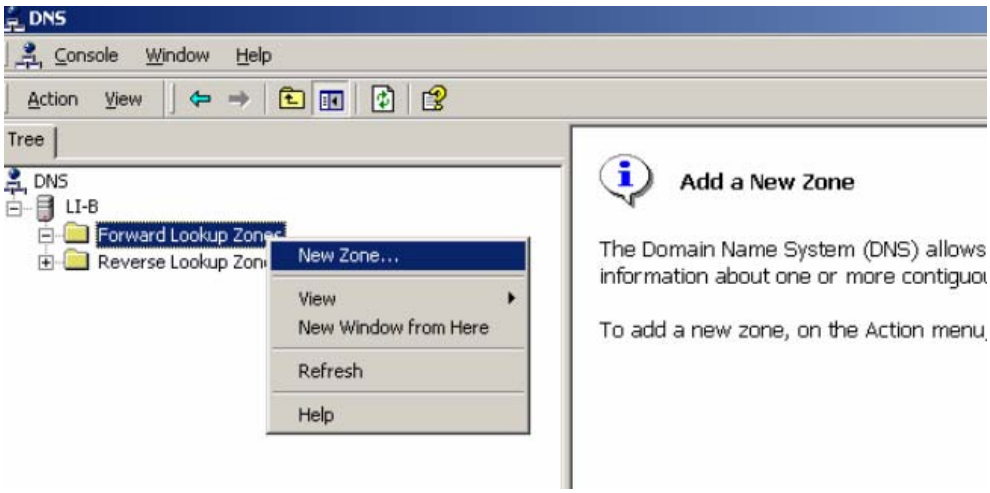
# Enter DNS server configuration page.

Select **Start** > **Programs** > **Administrative Tools** > **DNS**.

# Create zone com.

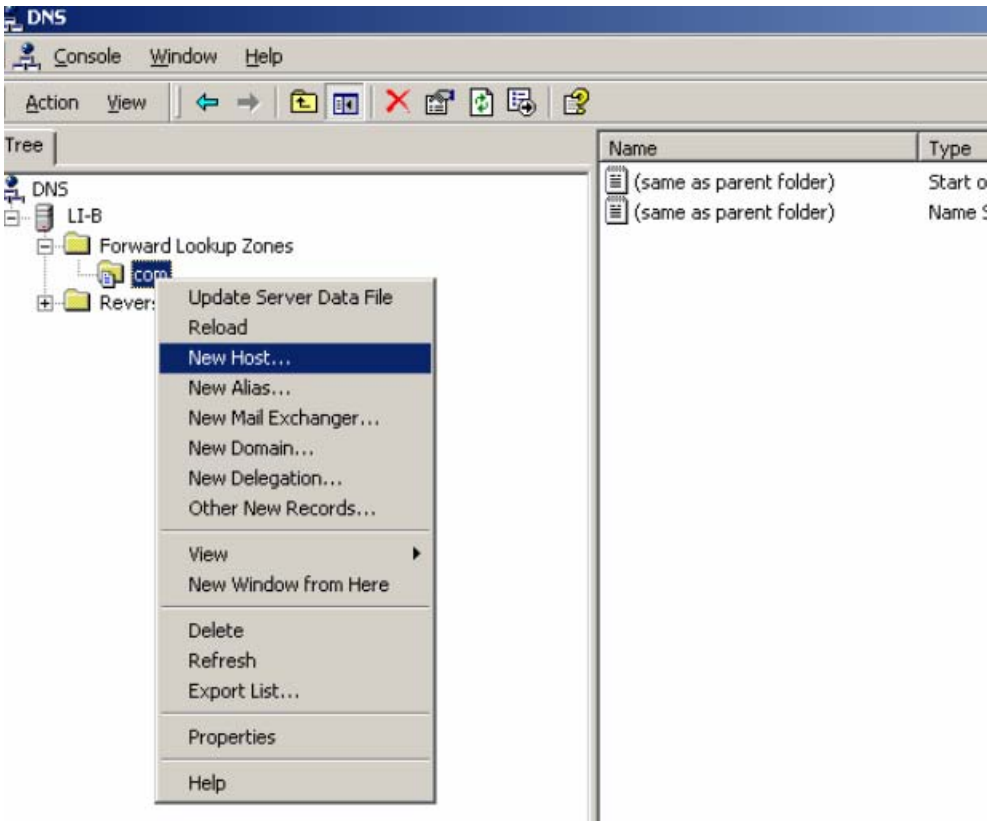
In Figure 1-5, right click **Forward Lookup Zones**, select **New zone**, and then follow the instructions to create a new zone named **com**.

**Figure 1-5** Create a zone



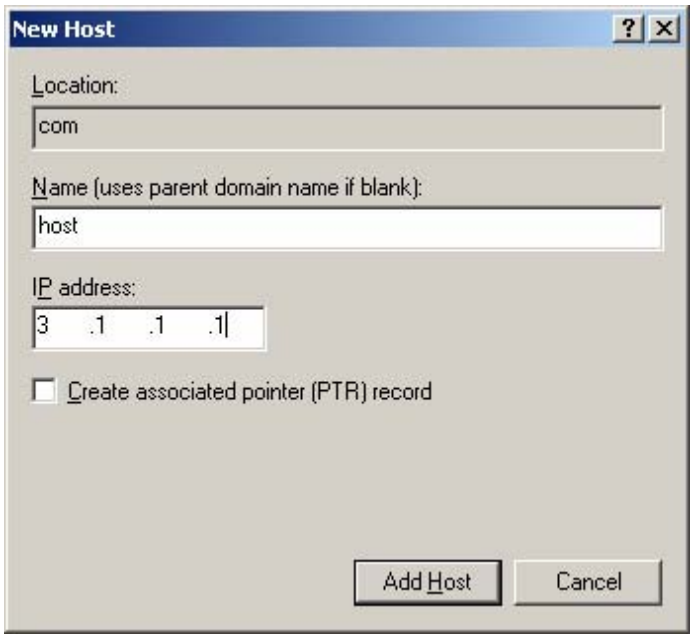

# Create a mapping between the host name and IP address.

**Figure 1-6** Add a host




In Figure 1-6, right click zone **com**, and then select **New Host** to bring up a dialog box as shown in Figure 1-7. Enter host name host and IP address 3.1.1.1.

**Figure 1-7** Add a mapping between domain name and IP address




2) Configure the DNS client

# Enable dynamic domain name resolution.

```
<Sysname> system-view
[Sysname] dns resolve
```

# Specify the DNS server 2.1.1.2.

```
[Sysname] dns server 2.1.1.2
```

# Configure com as the name suffix.

```
[Sysname] dns domain com
```

3) Configuration verification

# Execute the **ping host** command on the Switch to verify that the communication between the Switch and the host is normal and that the corresponding destination IP address is 3.1.1.1.

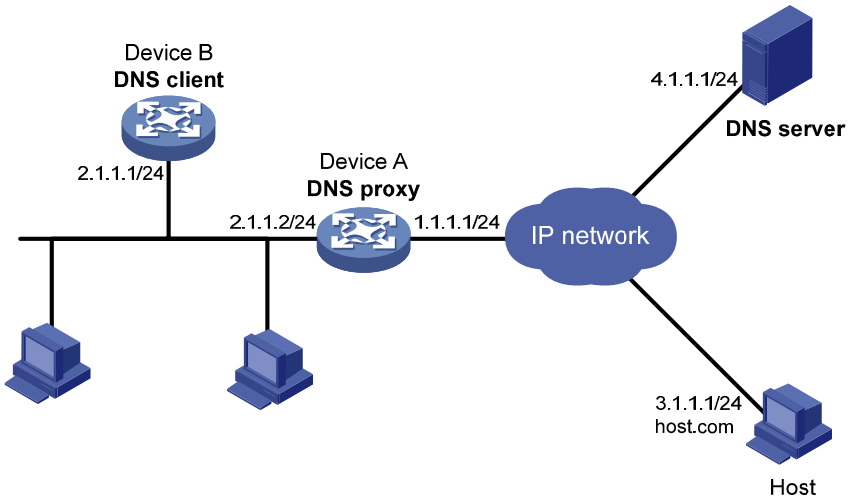
```
[Sysname] ping host
 Trying DNS resolve, press CTRL_C to break
 Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1):
  56  data bytes, press CTRL_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

   --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

## DNS Proxy Configuration Example

### Network requirements

- Specify Switch A as the DNS server of Switch B (the DNS client).
- Switch A acts as a DNS proxy. The IP address of the real DNS server is 4.1.1.1.
- Switch B implements domain name resolution through Switch A.

**Figure 1-8** Network diagram for DNS proxy




### Configuration procedure

---

**Note**

Before performing the following configuration, assume that Switch A, the DNS server, and the host are reachable to each other and the IP addresses of the interfaces are configured as shown in Figure 1-8.

---

1) Configure the DNS server

This configuration may vary with different DNS servers. When a Windows server 2000 acts as the DNS server, refer to Dynamic Domain Name Resolution Configuration Example for related configuration information.

2) Configure the DNS proxy

# Specify the DNS server 4.1.1.1.

```
<SwitchA> system-view
[SwitchA] dns server 4.1.1.1
```

# Enable DNS proxy.

```
[SwitchA] dns proxy enable
```

3) Configure the DNS client

# Enable the domain name resolution function.

```
<SwitchB> system-view
[SwitchB] dns resolve
```

# Specify the DNS server 2.1.1.2.

```
[SwitchB] dns server 2.1.1.2
```

4) Configuration verification

# Execute the **ping host.com** command on Switch B to verify that the communication between the Switch and the host is normal and that the corresponding destination IP address is 3.1.1.1.

```
[SwitchB] ping host.com
Trying DNS resolve, press CTRL_C to break
 Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1):
  56  data bytes, press CTRL_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

# Troubleshooting DNS Configuration

## Symptom

After enabling the dynamic domain name resolution, the user cannot get the correct IP address.

## Solution

- Use the **display dns dynamic-host** command to verify that the specified domain name is in the cache.
- If the specified domain name does not exist, check that dynamic domain name resolution is enabled and the DNS client can communicate with the DNS server.
- If the specified domain name is in the cache, but the IP address is incorrect, check that the DNS client has the correct IP address of the DNS server.
- Verify the mapping between the domain name and IP address is correct on the DNS server.

# Table of Contents

# 1 IP Performance Optimization Configuration

When optimizing IP performance, go to these sections for information you are interested in:



## IP Performance Overview

In some network environments, you can adjust the IP parameters to achieve best network performance. IP performance optimization configuration includes:

- Enabling the device to receive and forward directed broadcasts
- Configuring TCP timers
- Configuring the TCP buffer size
- Enabling ICMP error packets sending

## Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network

Directed broadcast packets are broadcast on a specific network. In the destination IP address of a directed broadcast, the network ID is a network ID identifies the target network, and the host ID is all-one. If a device is allowed to forward directed broadcasts to a directly connected network, hackers may mount attacks to the network. Therefore, the device is disabled from receiving and forwarding directed broadcasts to a directly connected network by default. However, you should enable the feature when using the Wake on LAN function to forward directed broadcasts to a host on the remote network.

### Enabling Reception of Directed Broadcasts to a Directly Connected Network

If a device is enabled to receive directed broadcasts, the device will determine whether to forward them according to the configuration on the outgoing interface.

Follow these steps to enable the device to receive directed broadcasts:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the device to receive directed broadcasts | **ip forward-broadcast** | Required<br>By default, the device is disabled from receiving directed broadcasts. |

## Enabling Forwarding of Directed Broadcasts to a Directly Connected Network

Follow these steps to enable the device to forward directed broadcasts:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the interface to forward directed broadcasts | **ip forward-broadcast** [ **acl** *acl-number* ] | Required<br>By default, the device is disabled from forwarding directed broadcasts. |

**Note**

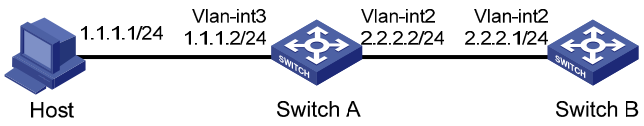
- If an ACL is referenced in the **ip forward-broadcast** [ *acl-number* ] command, only packets permitted by the ACL can be forwarded.
- If you repeatedly execute the **ip forward-broadcast acl** [ *acl-number* ] command on an interface, the last executed command takes effect only. If the command executed last time does not include the **acl** *acl-number*, the ACL configured previously will be removed.

## Configuration Example

### Network requirements

As shown in Figure 1-1, the host's interface and VLAN-interface 3 of Switch A are on the same network segment (1.1.1.0/24). VLAN-interface 2 of Switch A and VLAN-interface 2 of Switch B are on another network segment (2.2.2.0/24). The default gateway of the host is VLAN-interface 3 (IP address 1.1.1.2/24) of Switch A. Configure a static route on Switch B to enable the reachability between host and Switch B.

**Figure 1-1** Network diagram for receiving and forwarding directed broadcasts




### Configuration procedure

- Configure Switch A

# Enable Switch A to receive directed broadcasts.

```
<SwitchA> system-view
[SwitchA] ip forward-broadcast
```

# Configure IP addresses for VLAN-interface 3 and VLAN-interface 2.

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
```

```
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

# Enable VLAN-interface 2 to forward directed broadcasts.

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

- Configure Switch B

# Enable Switch B to receive directed broadcasts.

```
<SwitchB> system-view
[SwitchB] ip forward-broadcast
```

# Configure a static route to the host.

```
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

# Configure an IP address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

After the above configurations, if you ping the subnet broadcast address (2.2.2.255) of VLAN-interface 2 of Switch A on the host, the ping packets can be received by VLAN-interface 2 of Switch B. However, if you disable the **ip forward-broadcast** command, the ping packets cannot be received by the VLAN-interface 2 of Switch B.

## Configuring TCP Optional Parameters

TCP optional parameters that can be configured include:

- synwait timer: When sending a SYN packet, TCP starts the synwait timer. If no response packet is received within the synwait timer interval, the TCP connection cannot be created.
- finwait timer: When a TCP connection is changed into FIN_WAIT_2 state, the finwait timer is started. If no FIN packets is received within the timer interval, the TCP connection will be terminated. If a FIN packet is received, the TCP connection state changes to TIME_WAIT. If a non-FIN packet is received, the system restarts the timer upon receiving the last non-FIN packet. The connection is broken after the timer expires.
- Size of TCP receive/send buffer

Follow these steps to configure TCP optional parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the TCP synwait timer | **tcp timer syn-timeout** *time-value* | Optional<br>75 seconds by default. |
| Configure the TCP finwait timer | **tcp timer fin-timeout** *time-value* | Optional<br>675 seconds by default. |
| Configure the size of TCP receive/send buffer | **tcp window** *window-size* | Optional<br>8 KB by default. |

**Caution**

The actual length of the finwait timer is determined by the following formula:
Actual length of the finwait timer = (Configured length of the finwait timer – 75) + configured length of the synwait timer

# Configuring ICMP to Send Error Packets

Sending error packets is a major function of ICMP. In case of network abnormalities, ICMP packets are usually sent by the network or transport layer protocols to notify corresponding devices so as to facilitate control and management.

## Advantages of sending ICMP error packets

There are three kinds of ICMP error packets: redirect packets, timeout packets and destination unreachable packets. Their sending conditions and functions are as follows.

1) Sending ICMP redirect packets

A host may have only a default route to the default gateway in its routing table after startup. The default gateway will send ICMP redirect packets to the source host, telling it to reselect a correct next hop to send the subsequent packets, if the following conditions are satisfied:

- The receiving and forwarding interfaces are the same.
- The selected route has not been created or modified by ICMP redirect packet.
- The selected route is not the default route of the device.
- There is no source route option in the packet.

ICMP redirect packets function simplifies host administration and enables a host to gradually establish a sound routing table to find out the best route.

2) Sending ICMP timeout packets

If the device received an IP packet with a timeout error, it drops the packet and sends an ICMP timeout packet to the source.

The device will send an ICMP timeout packet under the following conditions:

- If the device finds the destination of a packet is not itself and the TTL field of the packet is 1, it will send a “TTL timeout” ICMP error message.
- When the device receives the first fragment of an IP datagram whose destination is the device itself, it starts a timer. If the timer times out before all the fragments of the datagram are received, the device will send a “reassembly timeout” ICMP error packet.

3) Sending ICMP destination unreachable packets

If the device receives an IP packet with the destination unreachable, it will drop the packet and send an ICMP destination unreachable error packet to the source.

Conditions for sending this ICMP packet:

- If neither a route nor the default route for forwarding a packet is available, the device will send a “network unreachable” ICMP error packet.
- If the destination of a packet is local while the transport layer protocol of the packet is not supported by the local device, the device sends a “protocol unreachable” ICMP error packet to the source.

- When receiving a packet with the destination being local and transport layer protocol being UDP, if the packet's port number does not match the running process, the device will send the source a "port unreachable" ICMP error packet.
- If the source uses "strict source routing" to send packets, but the intermediate device finds that the next hop specified by the source is not directly connected, the device will send the source a "source routing failure" ICMP error packet.
- When forwarding a packet, if the MTU of the sending interface is smaller than the packet but the packet has been set "Don't Fragment", the device will send the source a "fragmentation needed and Don't Fragment (DF)-set" ICMP error packet.

### Disadvantages of sending ICMP error packets

Although sending ICMP error packets facilitates network control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If a device receives a lot of malicious packets that cause it to send ICMP error packets, its performance will be reduced.
- As the redirection function increases the routing table size of a host, the host's performance will be reduced if its routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

To prevent such problems, you can disable the device from sending ICMP error packets.

Follow these steps to disable sending of ICMP error packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable sending of ICMP redirect packets | **ip redirects enable** | Required<br>Disabled by default. |
| Disable sending of ICMP timeout packets | **undo ip ttl-expires** | Required<br>Enabled by default. |
| Enable sending of ICMP destination unreachable packets | **ip unreachables enable** | Required<br>Disabled by default. |

**Note**

The device stops sending "TTL timeout" ICMP error packets after sending ICMP timeout packets is disabled. However, "reassembly timeout" error packets will be sent normally.

# Displaying and Maintaining IP Performance Optimization

| To do… | Use the command… | Remarks |
|---|---|---|
| Display current TCP connection state | **display tcp status** | Available in any view |
| Display TCP connection statistics | **display tcp statistics** | |
| Display UDP statistics | **display udp statistics** | |
| Display statistics of IP packets | **display ip statistics** | |
| Display statistics of ICMP flows | **display icmp statistics** | |
| Display socket information | **display ip socket** [ **socktype** *sock-type* ] [ *task-id socket-id* ] | |
| Display FIB information | **display fib** [ **\|** { **begin** \| **include** \| **exclude** } *regular-expression* \| **acl** *acl-number* \| **ip-prefix** *ip-prefix-name* ] | |
| Display FIB information matching the specified destination IP address | **display fib** *ip-address* [ *mask* \| *mask-length* ] | |
| Clear statistics of IP packets | **reset ip statistics** | Available in user view |
| Clear statistics of TCP connections | **reset tcp statistics** | Available in user view |
| Clear statistics of UDP traffic | **reset udp statistics** | Available in user view |

# Table of Contents

# 1 UDP Helper Configuration

When configuring UDP Helper, go to these sections for information you are interested in:



**Note**

UDP Helper can be currently configured on VLAN interfaces only.

## Introduction to UDP Helper

Sometimes, a host needs to forward broadcasts to obtain network configuration information or request the names of other devices on the network. However, if the server or the device to be requested is located in another broadcast domain, the host cannot obtain such information through broadcast.

To solve this problem, the device provides the UDP Helper function to relay specified UDP packets. In other words, UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

With UDP Helper enabled, the device decides whether to forward a received UDP broadcast packet according to the UDP destination port number of the packet.

- If the destination port number of the packet matches the one pre-configured on the device, the device modifies the destination IP address in the IP header, and then sends the packet to the specified destination server.
- If not, the device sends the packet to the upper layer protocol for processing.

## Configuring UDP Helper

Follow these steps to configure UDP Helper:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable UDP Helper | **udp-helper enable** | Required<br>Disabled by default. |
| Enable the forwarding of packets with the specified UDP destination port number(s) | **udp-helper port** { *port-number* \| **dns** \| **netbios-ds** \| **netbios-ns** \| **tacacs** \| **tftp** \| **time** } | Required<br>No UDP port number is specified by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter interface view | **interface** *interface-type interface-number* | — |
| Specify the destination server to which UDP packets are to be forwarded | **udp-helper server** *ip-address* | Required<br>No destination server is specified by default. |

**Caution**

- The UDP Helper enabled device cannot forward DHCP broadcast packets. That is to say, the UDP port number cannot be set to 67 or 68.
- For the **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords, you can specify port numbers or the corresponding parameters. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same UDP port number.
- The configuration of all UDP ports is removed if you disable UDP Helper.
- You can configure up to 256 UDP port numbers to enable the forwarding of packets with these UDP port numbers.
- You can configure up to 20 destination servers on an interface.

# Displaying and Maintaining UDP Helper

| To do… | Use the command… | Remarks |
|---|---|---|
| Displays the information of forwarded UDP packets | **display udp-helper server** [ **interface** *interface-type interface-number* ] | Available in any view |
| Clear statistics about packets forwarded | **reset udp-helper packet** | Available in user view |

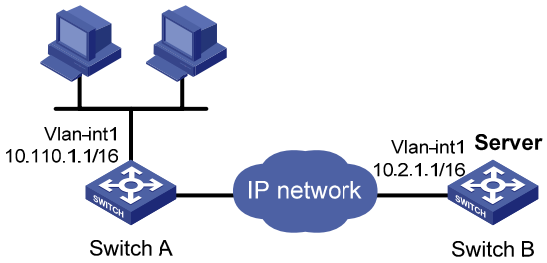
# UDP Helper Configuration Examples

## UDP Helper Configuration Example

### Network requirements

On Switch A, configure UDP helper to forward broadcast packets (with UDP destination port number 55 and destination IP address 255.255.255.255 or 10.110.255.255 to the destination server 10.2.1.1/16.

**Figure 1-1** Network diagram for UDP Helper configuration




## Configuration procedure

---

**Note**

The following configuration assumes that a route from Switch A to the network segment 10.2.0.0/16 is available.

---

# Enable UDP Helper.

```
<SwitchA> system-view
[SwitchA] udp-helper enable
```

# Enable the forwarding broadcast packets with the UDP destination port 55.

```
[SwitchA] udp-helper port 55
```

# Specify the destination server 10.2.1.1 on VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
[SwitchA-Vlan-interface1] udp-helper server 10.2.1.1
```

# Table of Contents

# 1 IPv6 Basics Configuration

When configuring IPv6 basics, go to these sections for information you are interested in:



**Note**

The term “router” or the router icon in this document refers to a router in a generic sense or a Layer 3 Ethernet switch running a routing protocol.

## IPv6 Overview

Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits. This section covers the following:



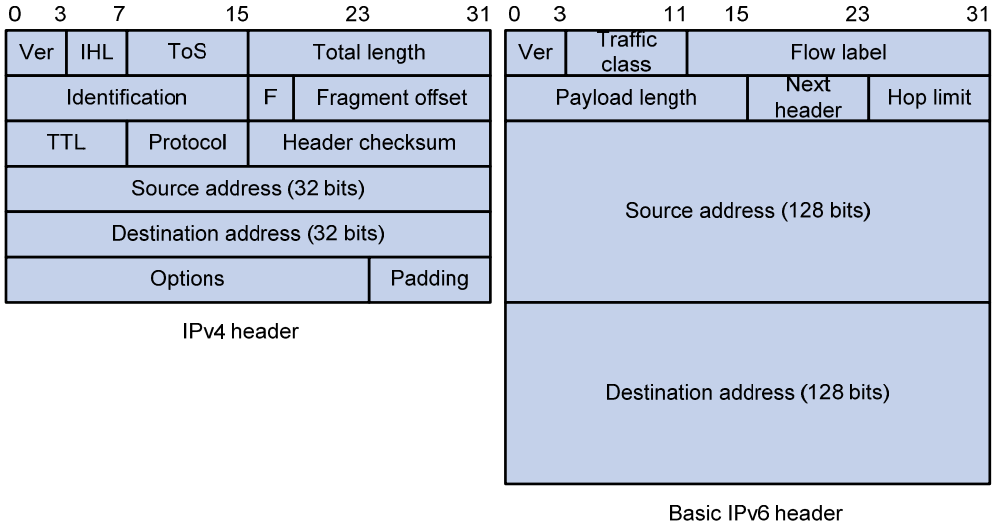
### IPv6 Features

#### Header format simplification

IPv6 cuts down some IPv4 header fields or move them to the IPv6 extension headers to reduce the length of the basic IPv6 header. IPv6 uses the basic header with a fixed length, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times

the IPv4 address size, the basic IPv6 header size is 40 bytes and is only twice the IPv4 header size (excluding the Options field).

**Figure 1-1** Comparison between IPv4 packet header format and basic IPv6 packet header format




### Adequate address space

The source and destination IPv6 addresses are both 128 bits (16 bytes) long. IPv6 can provide 3.4 x $10^{38}$ addresses to fully meet the requirements of hierarchical address division as well as allocation of public and private addresses.

### Hierarchical address structure

IPv6 adopts the hierarchical address structure to quicken route search and reduce the system sources occupied by the IPv6 routing table by route aggregation.

### Automatic address configuration

To simplify host configuration, IPv6 supports stateful and stateless address configuration.

- Stateful address configuration means that a host acquires an IPv6 address and related information from a server (for example, a DHCP server).
- Stateless address configuration means that a host automatically generates an IPv6 address and related information on the basis of its own link-layer address and the prefix information advertised by a router.

In addition, a host can generate a link-local address on the basis of its own link-layer address and the default prefix (FE80::/10) to communicate with other hosts on the same link.

### Built-in security

IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and enhances the interoperability between different IPv6 applications.

### QoS support

The Flow Label field in the IPv6 header allows the device to label packets of a flow and provide special handling for these packets.

### Enhanced neighbor discovery mechanism

The IPv6 neighbor discovery protocol is implemented through a group of Internet Control Message Protocol Version 6 (ICMPv6) messages that manage the information exchange between neighbor nodes on the same link. The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP) messages, Internet Control Message Protocol version 4 (ICMPv4) router discovery messages, and ICMPv4 redirection messages and provides a series of other functions.

### Flexible extension headers

IPv6 cancels the Options field in the IPv4 header but introduces multiple extension headers to provide scalability while improving efficiency. The Options field contains 40 bytes at most, while the size of IPv6 extension headers is restricted to the maximum size of IPv6 packets.

## Introduction to IPv6 Address

### IPv6 address format

An IPv6 address is represented as a set of 16-bit hexadecimals, separated by colons. An IPv6 address is divided into eight groups, and the 16 bits of each group are represented by four hexadecimal numbers, for example, 2001:0000:130F:0000:0000:09C0:876A:130B.

To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

- Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in a shorter format as 2001:0:130F:0:0:9C0:876A:130B.
- If an IPv6 address contains two or more consecutive groups of zeros, they can be replaced by a double-colon ::. For example, the above-mentioned address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.

---

**Caution**

A double-colon can be used only once in an IPv6 address. Otherwise, the device is unable to determine how many zeros that double-colons represent when converting them to zeros to restore a 128-bit IPv6 address.

---

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation, where the IPv6-address is in any of the notations above mentioned, and prefix-length is a decimal number indicating how many bits from the left-most of an IPv6 address is the address prefix.

### IPv6 address classification

IPv6 addresses fall into three types: unicast address, multicast address, and anycast address.

- Unicast address: An identifier for a single interface, similar to an IPv4 unicast address. A packet sent to a unicast address is delivered to the interface identified by that address.
- Multicast address: An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address.

- Anycast address: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the target interface is nearest to the source, according to a routing protocol's measure of distance).

---

**Note**

There are no broadcast addresses in IPv6. Their function is replaced by multicast addresses.

---

The type of an IPv6 address is designated by the first several bits called format prefix. Table 1-1 lists the mappings between address types and format prefixes.

**Table 1-1** Mappings between address types and format prefixes

| Type | | Format prefix (binary) | IPv6 prefix ID |
|---|---|---|---|
| Unicast address | Unassigned address | 00...0 (128 bits) | ::/128 |
| | Loopback address | 00...1 (128 bits) | ::1/128 |
| | Link-local address | 1111111010 | FE80::/10 |
| | Site-local address | 1111111011 | FEC0::/10 |
| | Global unicast address | other forms | — |
| Multicast address | | 11111111 | FF00::/8 |
| Anycast address | | Anycast addresses are taken from unicast address space and are not syntactically distinguishable from unicast addresses. | |

## Unicast address

There are several types of unicast addresses, including aggregatable global unicast address, link-local address, and site-local address.

- The aggregatable global unicast addresses, equivalent to public IPv4 addresses, are provided for network service providers. This type of address allows efficient prefix aggregation to restrict the number of global routing entries.
- The link-local addresses are used for communication between link-local nodes in neighbor discovery and stateless autoconfiguration. Packets with link-local source or destination addresses are not forwarded to other links.
- IPv6 unicast site-local addresses are similar to private IPv4 addresses. Packets with site-local source or destination addresses are not forwarded out of the local site (a private network).
- Loopback address: The unicast address 0:0:0:0:0:0:0:1 (represented in the shortest format as ::1) is called the loopback address and may never be assigned to any physical interface. Like the loopback address in IPv4, it may be used by a node to send an IPv6 packet to itself.
- Unassigned address: The unicast address "::" is called the unassigned address and may not be assigned to any node. Before acquiring a valid IPv6 address, a node may fill this address in the source address field of an IPv6 packet. It cannot be used as a destination IPv6 address.

### Multicast address

IPv6 multicast addresses listed in Table 1-2 are reserved for special purpose.

**Table 1-2** Reserved IPv6 multicast addresses

| Address | Application |
|---|---|
| FF01::1 | Node-local scope all nodes multicast address |
| FF02::1 | Link-local scope all nodes multicast address |
| FF01::2 | Node-local scope all routers multicast address |
| FF02::2 | Link-local scope all routers multicast address |
| FF05::2 | Site-local scope all routers multicast address |

Besides, there is another type of multicast address: solicited-node address. A solicited-node multicast address is used to acquire the link-layer address of a neighbor node on the same link, and is also used for duplicate address detection (DAD). Each IPv6 unicast or anycast address has a corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

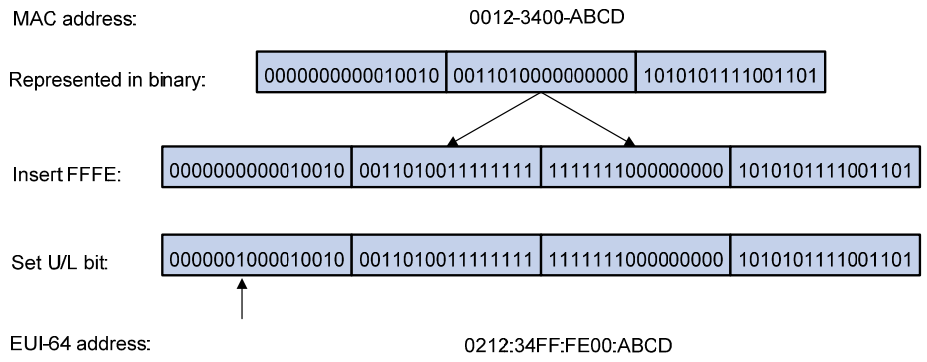
FF02:0:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:0:1:FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 unicast or anycast address.

### Interface identifier in IEEE EUI-64 format

An interface identifier is used to identify a unique interface on a link and is 64 bits long. An interface identifier in IEEE EUI-64 format is derived from the link-layer address (MAC) of an interface. A MAC address is 48 bits long and therefore, to get the interface identifier, the hexadecimal number FFFE needs to be inserted in the middle of the MAC address (behind the 24 high-order bits). To ensure the interface identifier obtained from a MAC address is unique, it is necessary to set the universal/local (U/L) bit (the seventh high-order bit) to “1”. Thus, an interface identifier in IEEE EUI-64 format is obtained.

**Figure 1-2** Convert a MAC address into an EUI-64 interface identifier




## Introduction to IPv6 Neighbor Discovery Protocol

The IPv6 Neighbor Discovery Protocol (NDP) uses five types of ICMPv6 messages to implement the following functions:

- Address resolution
- Neighbor reachability detection

- Duplicate address detection
- Router/prefix discovery and address autoconfiguration
- Redirection

Table 1-3 lists the types and functions of ICMPv6 messages used by the NDP.

**Table 1-3** Types and functions of ICMPv6 messages

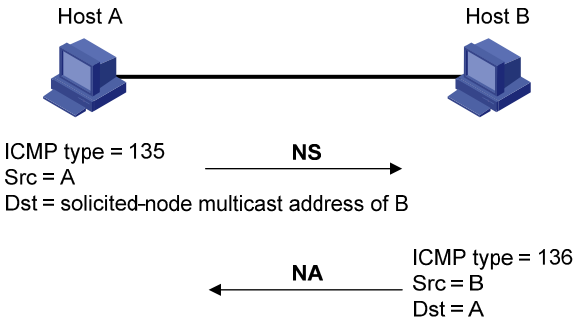
| ICMPv6 message | Number | Function |
|---|---|---|
| Neighbor solicitation (NS) message | 135 | Used to acquire the link-layer address of a neighbor |
| | | Used to verify whether the neighbor is reachable |
| | | Used to perform a duplicate address detection |
| Neighbor advertisement (NA) message | 136 | Used to respond to an NS message |
| | | When the link layer changes, the local node initiates an NA message to notify neighbor nodes of the node information change. |
| Router solicitation (RS) message | 133 | After started, a node sends an RS message to request the router for an address prefix and other configuration information for the purpose of autoconfiguration. |
| Router advertisement (RA) message | 134 | Used to respond to an RS message |
| | | With the RA message suppression disabled, the router regularly sends an RA message containing information such as prefix information options and flag bits. |
| Redirect message | 137 | When a certain condition is satisfied, the default gateway sends a redirect message to the source host so that the host can reselect a correct next hop router to forward packets. |

The NDP mainly provides the following functions:

## Address resolution

Similar to the ARP function in IPv4, a node acquires the link-layer addresses of neighbor nodes on the same link through NS and NA messages. Figure 1-3 shows how node A acquires the link-layer address of node B.

**Figure 1-3** Address resolution




The address resolution procedure is as follows:

1) Node A multicasts an NS message. The source address of the NS message is the IPv6 address of the sending interface of node A and the destination address is the solicited-node multicast address of node B. The NS message contains the link-layer address of node A.

2) After receiving the NS message, node B judges whether the destination address of the packet is its solicited-node multicast address. If yes, node B learns the link-layer address of node A, and then unicasts an NA message containing its link-layer address.
3) Node A acquires the link-layer address of node B from the NA message.

### Neighbor reachability detection

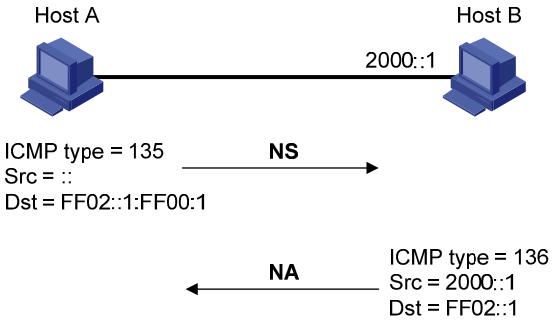
After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

1) Node A sends an NS message whose destination address is the IPv6 address of node B.
2) If node A receives an NA message from node B, node A considers that node B is reachable. Otherwise, node B is unreachable.

### Duplicate address detection

After node A acquires an IPv6 address, it will perform duplicate address detection (DAD) to determine whether the address is being used by any other node (similar to the gratuitous ARP function of IPv4). DAD is accomplished through NS and NA messages. Figure 1-4 shows the DAD procedure.

**Figure 1-4** Duplicate address detection




The DAD procedure is as follows:

1) Node A sends an NS message whose source address is the unassigned address :: and destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message contains the IPv6 address.
2) If node B uses this IPv6 address, node B returns an NA message. The NA message contains the IPv6 address of node B.
3) Node A learns that the IPv6 address is being used by node B after receiving the NA message from node B. Otherwise, node B is not using the IPv6 address and node A can use it.

### Router/prefix discovery and address autoconfiguration

Router/prefix discovery means that a node locates the neighboring routers, and learns the prefix of the network where the host is located, and other configuration parameters from the received RA message.

Stateless address autoconfiguration means that a node automatically generates an IPv6 address according to the information obtained through router/prefix discovery.

The router/prefix discovery is implemented through RS and RA messages. The router/prefix discovery procedure is as follows:

1) After started, a node sends an RS message to request the router for the address prefix and other configuration information for the purpose of autoconfiguration.

2) The router returns an RA message containing information such as prefix information option. (The router also regularly sends an RA message.)
3) The node automatically generates an IPv6 address and other information for its interface according to the address prefix and other configuration parameters in the RA message.

---

**Note**

- In addition to an address prefix, the prefix information option also contains the preferred lifetime and valid lifetime of the address prefix. After receiving a periodic RA message, the node updates the preferred lifetime and valid lifetime of the address prefix accordingly.
- An automatically generated address is applicable within the valid lifetime and is removed when the valid lifetime times out.

---

### Redirection

When a host is started, its routing table may contain only the default route to the gateway. When certain conditions are satisfied, the gateway sends an ICMPv6 redirect message to the source host so that the host can select a better next hop to forward packets (similar to the ICMP redirection function in IPv4).

The gateway sends an IPv6 ICMP redirect message when the following conditions are satisfied:

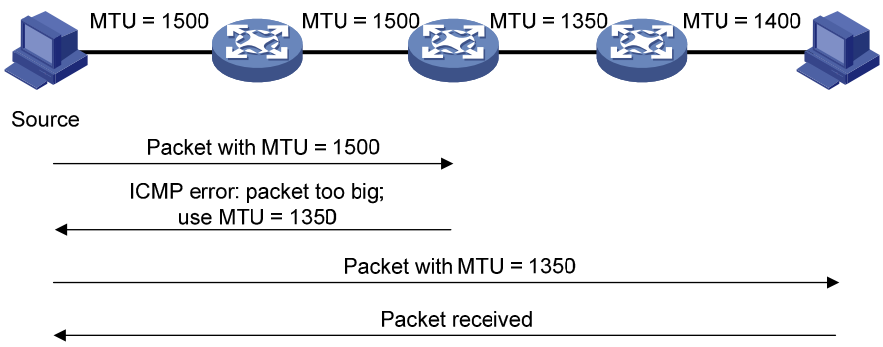
- The receiving interface is the forwarding interface.
- The selected route itself is not created or modified by an IPv6 ICMP redirect message.
- The selected route is not the default route.
- The forwarded IPv6 packet does not contain any routing extension header.

## IPv6 PMTU Discovery

The links that a packet passes from the source to the destination may have different MTUs. In IPv6, when the packet size exceeds the path MTU ( the minimum MTU of all links), the packet will be fragmented at the source end so as to reduce the processing pressure of forwarding devices and utilize network resources properly.

The path MTU (PMTU) discovery mechanism is to find the minimum MTU of all links in the path from the source to the destination. Figure 1-5 shows the working procedure of PMTU discovery.

**Figure 1-5** Working procedure of PMTU discovery




The working procedure of the PMTU discovery is as follows:

1) The source host uses its MTU to send packets to the destination host.
2) If the MTU supported by a forwarding interface is smaller than the packet size, the forwarding device will discard the packet and return an ICMPv6 error packet containing the interface MTU to the source host.
3) After receiving the ICMPv6 error packet, the source host uses the returned MTU to send packets to the destination.
4) Step 2 to step 3 are repeated until the destination host receives the packet. In this way, the minimum MTU of all links in the path from the source host to the destination host is determined.

### Introduction to IPv6 DNS

IPv6 Domain Name System (DNS) is responsible for translating domain names into IPv6 addresses, instead of IPv4 addresses.

Like IPv4 DNS, IPv6 DNS also involves static domain name resolution and dynamic domain name resolution. The function and implementation of these two types of domain name resolution are the same as those of IPv4 DNS. For details, refer to *DNS Configuration* in the *IP Services Volume*.

Usually, the DNS server connecting IPv4 and IPv6 networks not only contains A records (IPv4 addresses), but also AAAA records (IPv6 addresses). The DNS server can convert domain names into IPv4 addresses or IPv6 addresses. In this way, the DNS server implements the functions of both IPv6 DNS and IPv4 DNS.

### Protocols and Standards

Protocols and standards related to IPv6 include:

- RFC 1881: IPv6 Address Allocation Management
- RFC 1887: An Architecture for IPv6 Unicast Address Allocation
- RFC 1981: Path MTU Discovery for IP version 6
- RFC 2375: IPv6 Multicast Address Assignments
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526: Reserved IPv6 Subnet Anycast Addresses
- RFC 3307: Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596: DNS Extensions to Support IP Version 6

## IPv6 Basics Configuration Task List

Complete the following tasks to perform IPv6 basics configuration:

| Task | Remarks |
|---|---|
| Configuring Basic IPv6 Functions | Required |
| Configuring IPv6 NDP | Optional |
| Configuring PMTU Discovery | Optional |
| Configuring IPv6 TCP Properties | Optional |

| Task | Remarks |
|---|---|
| Configuring ICMPv6 Packet Sending | Optional |
| Configuring IPv6 DNS Client | Optional |

# Configuring Basic IPv6 Functions

## Enabling IPv6

Before performing IPv6-related configurations, you need to Enable IPv6. Otherwise, an interface cannot forward IPv6 packets even if it has an IPv6 address configured.

Follow these steps to Enable IPv6:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IPv6 | **ipv6** | Required<br>Disabled by default. |

## Configuring an IPv6 Unicast Address

IPv6 site-local addresses and aggregatable global unicast addresses can be configured in the following ways:

- EUI-64 format: When the EUI-64 format is adopted, the IPv6 address prefix of an interface is the configured prefix, and the interface identifier is derived from the link-layer address of the interface.
- Manual configuration: IPv6 site-local addresses or aggregatable global unicast addresses are configured manually.

IPv6 link-local addresses can be configured in either of the following ways:

- Automatic generation: The device automatically generates a link-local address for an interface according to the link-local address prefix (FE80::/10) and the link-layer address of the interface.
- Manual assignment: IPv6 link-local addresses can be assigned manually.

Follow these steps to configure an IPv6 unicast address:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view | | **interface** *interface-type interface-number* | — |
| Configure an IPv6 aggregatable global unicast address or site-local address | Manually assign an IPv6 address | **ipv6 address** { *ipv6-address prefix-length* \| *ipv6-address*/*prefix-length* } | One of the two commands is required.<br>By default, no site-local address or aggregatable global unicast address is configured for an interface. |
| | Adopt the EUI-64 format to form an IPv6 address | **ipv6 address** *ipv6-address*/*prefix-length* **eui-64** | |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Configure an IPv6 link-local address | Automatically generate a link-local address for the interface | **ipv6 address auto link-local** | Optional<br>By default, after an IPv6 site-local address or aggregatable global unicast address is configured for an interface, a link-local address will be generated automatically. |
| | Manually assign a link-local address for the interface | **ipv6 address** *ipv6-address* **link-local** | |

**Note**

- After an IPv6 site-local address or aggregatable global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command. If a link-local address is manually assigned to an interface, this manual link-local address takes effect. If the manually assigned link-local address is removed, the automatically generated link-local address takes effect.
- Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated.
- The **undo ipv6 address auto link-local** command can only remove the link-local addresses generated through the **ipv6 address auto link-local** command. However, if an IPv6 site-local address or aggregatable global unicast address is already configured for an interface, the interface still has a link-local address because the system automatically generates one for the interface. If no IPv6 site-local address or aggregatable global unicast address is configured, the interface has no link-local address.

# Configuring IPv6 NDP

## Configuring a Static Neighbor Entry

The IPv6 address of a neighbor node can be resolved into a link-layer address dynamically through NS and NA messages or through a manually configured static neighbor entry.

The device uniquely identifies a static neighbor entry according to the neighbor IPv6 address and the local Layer 3 interface ID. Currently, there are two configuration methods:

- Associate a neighbor IPv6 address and link-layer address with a Layer 3 interface.
- Associate a neighbor IPv6 address and link-layer address with a port in a VLAN.

Follow these steps to configure a static neighbor entry:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a static neighbor entry | **ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* \| **interface** *interface-type interface-number* } | Required |

**Caution**

You can adopt either of the two methods above to configure a static neighbor entry.

- After a static neighbor entry is configured by using the first method, the device needs to resolve the corresponding Layer 2 port information of the VLAN interface.
- If you adopt the second method, you should ensure that the corresponding VLAN interface exists and that the Layer 2 port specified by *port-type port-number* belongs to the VLAN specified by *vlan-id*. After a static neighbor entry is configured, the device relates the VLAN interface to the IPv6 address to uniquely identify a static neighbor entry.

## Configuring the Maximum Number of Neighbors Dynamically Learned

The device can dynamically acquire the link-layer address of a neighbor node through NS and NA messages and add it into the neighbor table. Too large a neighbor table may reduce the forwarding performance of the device. You can restrict the size of the neighbor table by setting the maximum number of neighbors that an interface can dynamically learn. When the number of dynamically learned neighbors reaches the threshold, the interface will stop learning neighbor information.

Follow these steps to configure the maximum number of neighbors dynamically learned:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure the maximum number of neighbors dynamically learned by an interface | **ipv6 neighbors max-learning-num** *number* | Optional<br>The default value is 1024. |

## Configuring Parameters Related to RA Messages

You can enable an interface to send RA messages, and configure the interval for sending RA messages and parameters in RA messages. After receiving an RA message, a host can use these parameters to perform corresponding operations. Table 1-4 lists the configurable parameters in an RA message and their descriptions.

**Table 1-4** Parameters in an RA message and their descriptions

| Parameters | Description |
|---|---|
| Cur hop limit | When sending an IPv6 packet, a host uses the value to fill the Cur Hop Limit field in IPv6 headers. The value is also filled into the Cur Hop Limit field in response messages of a device. |
| Prefix information options | After receiving the prefix information advertised by the device, the hosts on the same link can perform stateless autoconfiguration. |
| M flag | This field determines whether hosts use the stateful autoconfiguration to acquire IPv6 addresses.<br>If the M flag is set to 1, hosts use the stateful autoconfiguration to acquire IPv6 addresses (for example, through a DHCP server). Otherwise, hosts use the stateless autoconfiguration to acquire IPv6 addresses, that is, hosts generate IPv6 addresses according to their own link-layer addresses and the prefix information issued by the router. |
| O flag | This field determines whether hosts use the stateful autoconfiguration to acquire information other than IPv6 addresses.<br>If the O flag is set to 1, hosts use the stateful autoconfiguration to acquire information other than IPv6 addresses (for example, through a DHCP server). Otherwise, hosts use the stateless autoconfiguration to acquire information other than IPv6 addresses. |
| Router lifetime | This field is used to set the lifetime of the router that sends RA messages to serve as the default router of hosts. According to the router lifetime in the received RA messages, hosts determine whether the router sending RA messages can serve as the default router. |
| Retrans timer | If the device fails to receive a response message within the specified time after sending an NS message, the device will retransmit the NS message. |
| Reachable time | If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device needs to send a packet to a neighbor after the specified reachable time expires, the device will reconfirm whether the neighbor is reachable. |

**Note**

The values of the Retrans Timer and the Reachable Time configured for an interface are sent to hosts via RA messages. Furthermore, this interface sends NS messages at the interval of Retrans Timer and considers a neighbor reachable within the Reachable Time.

Follow these steps to configure parameters related to an RA message:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the hop limit | **ipv6 nd hop-limit** *value* | Optional<br>64 by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Disable the RA message suppression | **undo ipv6 nd ra halt** | Required<br>By default, RA messages are suppressed. |
| Configure the maximum and minimum intervals for sending RA messages | **ipv6 nd ra interval** *max-interval-value min-interval-value* | Optional<br>By default, the maximum interval for sending RA messages is 600 seconds, and the minimum interval is 200 seconds.<br>The device sends RA messages at random intervals between the maximum interval and the minimum interval.<br>The minimum interval should be less than or equal to 0.75 times the maximum interval. |
| Configure the prefix information in RA messages | **ipv6 nd ra prefix** { *ipv6-address prefix-length* \| *ipv6-address*/*prefix-length* } *valid-lifetime preferred-lifetime* [ **no-autoconfig** \| **off-link** ] * | Optional<br>By default, no prefix information is configured for RA messages, and the IPv6 address of the interface sending RA messages is used as the prefix information. |
| Set the M flag bit to 1 | **ipv6 nd autoconfig managed-address-flag** | Optional<br>By default, the M flag bit is set to 0, that is, hosts acquire IPv6 addresses through stateless autoconfiguration. |
| Set the O flag bit to 1 | **ipv6 nd autoconfig other-flag** | Optional<br>By default, the O flag bit is set to 0, that is, hosts acquire other information through stateless autoconfiguration. |
| Configure the router lifetime in RA messages | **ipv6 nd ra router-lifetime** *value* | Optional<br>1800 seconds by default. |
| Set the NS retransmission timer | **ipv6 nd ns retrans-timer** *value* | Optional<br>By default, the local interface sends NS messages at an interval of 1000 milliseconds, and the value of the Retrans Timer field in RA messages sent by the local interface is 0. |
| Set the reachable time | **ipv6 nd nud reachable-time** *value* | Optional<br>By default, the neighbor reachable time on the local interface is 30000 milliseconds, and the value of the Reachable Timer field in RA messages is 0. |

**Caution**

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

### Configuring the Maximum Number of Attempts to Send an NS Message for DAD

An interface sends a neighbor solicitation (NS) message for duplicate address detection after acquiring an IPv6 address. If the interface does not receive a response within a specified time (determined by the **ipv6 nd ns retrans-timer** command), it continues to send an NS message. If it still does not receive a response after the number of sent attempts reaches a configurable threshold, the acquired address is considered usable.

Follow these steps to configure the attempts to send an NS message for DAD:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure the number of attempts to send an NS message for DAD | **ipv6 nd dad attempts** *value* | Optional<br>1 by default. When the *value* argument is set to 0, DAD is disabled. |

## Configuring PMTU Discovery

### Configuring a Static PMTU for a Specified IPv6 Address

You can configure a static PMTU for a specified destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static PMTU of the specified destination IPv6 address. If the packet size is larger than the smaller one between the two values, the host fragments the packet according to the smaller value.

Follow these steps to configure a static PMTU for a specified address:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a static PMTU for a specified IPv6 address | **ipv6 pathmtu** *ipv6-address* [ *value* ] | Required<br>By default, no static PMTU is configured. |

### Configuring the Aging Time for Dynamic PMTUs

After the path MTU from a source host to a destination host is dynamically determined (refer to IPv6 PMTU Discovery), the source host sends subsequent packets to the destination host on basis of this MTU. After the aging time expires, the dynamic PMTU is removed and the source host re-determines a dynamic path MTU through the PMTU mechanism.

The aging time is invalid for a static PMTU.

Follow these steps to configure the aging time for dynamic PMTUs:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the aging time for dynamic PMTUs | **ipv6 pathmtu age** *age-time* | Optional<br>10 minutes by default. |

# Configuring IPv6 TCP Properties

The IPv6 TCP properties you can configure include:

- synwait timer: When a SYN packet is sent, the synwait timer is triggered. If no response packet is received before the synwait timer expires, the IPv6 TCP connection establishment fails.
- finwait timer: When the IPv6 TCP connection status is FIN_WAIT_2, the finwait timer is triggered. If no packet is received before the finwait timer expires, the IPv6 TCP connection is terminated. If a FIN packet is received, the IPv6 TCP connection status becomes TIME_WAIT. If non-FIN packets are received, the finwait timer is reset upon receipt of the last non-FIN packet and the connection is terminated after the finwait timer expires.
- Size of the IPv6 TCP sending/receiving buffer.

Follow these steps to configure IPv6 TCP properties:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the finwait timer | **tcp ipv6 timer fin-timeout** *wait-time* | Optional<br>675 seconds by default. |
| Set the synwait timer | **tcp ipv6 timer syn-timeout** *wait-time* | Optional<br>75 seconds by default. |
| Set the size of the IPv6 TCP sending/receiving buffer | **tcp ipv6 window** *size* | Optional<br>8 KB by default. |

# Configuring ICMPv6 Packet Sending

## Configuring the Maximum ICMPv6 Error Packets Sent in an Interval

If too many ICMPv6 error packets are sent within a short time in a network, network congestion may occur. To avoid network congestion, you can control the maximum number of ICMPv6 error packets sent within a specified time, currently by adopting the token bucket algorithm.

You can set the capacity of a token bucket, namely, the number of tokens in the bucket. In addition, you can set the update interval of the token bucket, namely, the interval for restoring the configured capacity. One token allows one ICMPv6 error packet to be sent. Each time an ICMPv6 error packet is sent, the number of tokens in a token bucket decreases by one. If the number of ICMPv6 error packets successively sent exceeds the capacity of the token bucket, the additional ICMPv6 error packets cannot be sent out until the capacity of the token bucket is restored.

Follow these steps to configure the capacity and update interval of the token bucket:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the capacity and update interval of the token bucket | **Ipv6 icmp-error** { **bucket** *bucket-size* \| **ratelimit** *interval* } * | Optional<br>By default, the capacity of a token bucket is 10 and the update interval is 100 milliseconds. That is, at most 10 IPv6 ICMP error packets can be sent within 100 milliseconds.<br>The update interval “0” indicates that the number of ICMPv6 error packets sent is not restricted. |

## Enable Sending of Multicast Echo Replies

If hosts are capable of answering multicast echo requests, Host A can attack Host B by sending an echo request with the source being Host B to a multicast address, then all the hosts in the multicast group will send echo replies to Host B. Therefore, to prevent such an attack, a device is disabled from replying multicast echo requests by default.

Follow these steps to enable sending of multicast echo replies:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable sending of multicast echo replies | **ipv6 icmpv6 multicast-echo-reply enable** | Not enabled by default. |

## Enabling Sending of ICMPv6 Time Exceeded Packets

A device sends an ICMPv6 time exceeded packet in the following cases.

- If a received IPv6 packet’s destination IP address is not the local address and its hop count is 1, the device sends an ICMPv6 time-to-live count exceeded packet to the source.
- Upon receiving the first fragment of an IPv6 datagram with the destination IP address being the local address, the device starts a timer. If the timer expires before all the fragments arrive, an ICMPv6 fragment reassembly time exceeded packet is sent to the source.

If large amounts of malicious packets are received, the performance of a device degrades greatly because it has to send back ICMP time exceeded packets. You can disable sending of ICMPv6 time-to-live count exceeded packets.

Follow these steps to enable sending of ICMPv6 time exceeded packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable sending of ICMPv6 time exceeded packets | **ipv6 hoplimit-expires enable** | Optional<br>Enabled by default. |

# Configuring IPv6 DNS Client

## Configuring Static IPv6 Domain Name Resolution

Configuring static IPv6 domain name resolution is to establish the mapping between a host name and an IPv6 address. When using such applications as Telnet, you can directly input a host name and the system will resolve the host name into an IPv6 address. Each host name can correspond to only one IPv6 address.

Follow these steps to configure static IPv6 domain name resolution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a host name to IPv6 address mapping | **ipv6 host** *hostname ipv6-address* | Required |

## Configuring Dynamic IPv6 Domain Name Resolution

You can use the following command to enable the dynamic domain name resolution function. In addition, you need to configure a DNS server so that a query request message can be sent to the correct server for resolution. The system can support at most six DNS servers.

You can configure a DNS suffix so that you only need to enter part of a domain name, and the system can automatically add the preset suffix for address resolution. The system can support at most 10 DNS suffixes.

Follow these steps to configure dynamic IPv6 domain name resolution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the dynamic domain name resolution function | **dns resolve** | Required<br>Disabled by default. |
| Configure an IPv6 DNS server | **dns server ipv6** *ipv6-address* [ *interface-type interface-number* ] | Required<br>If the IPv6 address of the DNS server is a link-local address, you need to specify the *interface-type* and *interface-number* argument. |
| Configure a DNS suffix | **dns domain** *domain-name* | Required<br>By default, no domain name suffix is configured, that is, the domain name is resolved according to the input information. |

**Note**

The **dns resolve** and **dns domain** commands are the same as those of IPv4 DNS. For details about the commands, refer to *DNS Commands* in the *IP Services Volume*.

# Displaying and Maintaining IPv6 Basics Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display DNS suffix information | **display dns domain** [ **dynamic** ] | Available in any view |
| Display IPv6 dynamic domain name cache information | **display dns ipv6 dynamic-host** | |
| Display IPv6 DNS server information | **display dns ipv6 server** [ **dynamic** ] | |
| Display the IPv6 FIB entries | **display ipv6 fib** [ *ipv6-address* ] | |
| Display the host name to IPv6 address mappings in the static DNS database | **display ipv6 host** | |
| Display the IPv6 interface settings | **display ipv6 interface** [ *interface-type* [ *interface-number* ] ] [ **verbose** ] | |
| Display neighbor information | **display ipv6 neighbors** { { *ipv6-address* \| **all** \| **dynamic** \| **static** } \| **interface** *interface-type interface-number* \| **vlan** *vlan-id* } [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | |
| Display the total number of neighbor entries satisfying the specified conditions | **display ipv6 neighbors** { { **all** \| **dynamic** \| **static** } \| **interface** *interface-type interface-number* \| **vlan** *vlan-id* } **count** | |
| Display the PMTU information of an IPv6 address | **display ipv6 pathmtu** { *ipv6-address* \| **all** \| **dynamic** \| **static** } | |
| Display socket information | **display ipv6 socket** [ **socktype** *socket-type* ] [ *task-id socket-id* ] | |
| Display the statistics of IPv6 packets and ICMPv6 packets | **display ipv6 statistics** | |
| Display the IPv6 TCP connection statistics | **display tcp ipv6 statistics** | |
| Display the IPv6 TCP connection status information | **display tcp ipv6 status** | |
| Display the IPv6 UDP connection statistics | **display udp ipv6 statistics** | |
| Clear IPv6 dynamic domain name cache information | **reset dns ipv6 dynamic-host** | Available in user view |
| Clear IPv6 neighbor information | **reset ipv6 neighbors** { **all** \| **dynamic** \| **interface** *interface-type interface-number* \| **static** } | |
| Clear the specified PMTU values | **reset ipv6 pathmtu** { **all** \| **static** \| **dynamic**} | |
| Clear the statistics of IPv6 and ICMPv6 packets | **reset ipv6 statistics** | |
| Clear all IPv6 TCP connection statistics | **reset tcp ipv6 statistics** | |
| Clear the statistics of all IPv6 UDP packets | **reset udp ipv6 statistics** | |

**Note**

The **display dns domain** command is the same as the one of IPv4 DNS. For details about the commands, refer to *DNS Commands* in the *IP Services Volume*.

# IPv6 Configuration Example

## Network requirements

- Host, Switch A and Switch B are directly connected through Ethernet ports. Add the Ethernet ports into corresponding VLANs, configure IPv6 addresses for the VLAN interfaces and verify the connectivity between them.
- The aggregatable global unicast addresses of VLAN-interface 2 and VLAN-interface 1 on Switch A are 3001::1/64 and 2001::1/64 respectively.
- The aggregatable global unicast address of VLAN-interface 2 on Switch B is 3001::2/64, and a route to Host is available.
- IPv6 is enabled for Host to automatically get an IPv6 address through IPv6 NDP, and a route to Switch B is available.

**Figure 1-6** Network diagram for IPv6 address configuration


**Note**

The VLAN interfaces have been created on the switch.

## Configuration procedure

- Configure Switch A

# Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Specify an aggregatable global unicast address for VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

# Specify an aggregatable global unicast address for VLAN-interface 1, and allow it to advertise RA messages (no interface advertises RA messages by default).

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
```

- Configure Switch B

# Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

# Configure an aggregatable global unicast address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
```

# Configure an IPv6 static route with destination IP address 2001::/64 and next hop address 3001::1.

```
[SwitchB-Vlan-interface2] ipv6 route-static 2001:: 64 3001::1
```

- Configure Host

Enable IPv6 for Host to automatically get an IPv6 address through IPv6 NDP.

```
[SwitchA-Vlan-interface1] display ipv6 neighbors interface gigabitethernet 1/0/2
                Type: S-Static    D-Dynamic
IPv6 Address                Link-layer      VID  Interface    State T Age
FE80::215:E9FF:FEA6:7D14    0015-e9a6-7d14   1   GE1/0/2      STALE D 1238
2001::15B:E0EA:3524:E791    0015-e9a6-7d14   1   GE1/0/2      STALE D 1248
```

The above information shows that the IPv6 aggregatable global unicast address that Host obtained is 2001::15B:E0EA:3524:E791.

## Verification

# Display the IPv6 interface settings on Switch A.

```
[SwitchA-Vlan-interface1] display ipv6 interface vlan-interface 2 verbose
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:2
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FF00:2
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   25829
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
```

```
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   47
  OutRequests:                  89
  OutForwDatagrams:             48
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  6
  InMcastNotMembers:            25747
  OutMcastPkts:                 48
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
[SwitchA-Vlan-interface1] display ipv6 interface vlan-interface 1 verbose
Vlan-interface1 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1C0
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FF00:1C0
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   272
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
```

```
  ReasmOKs:                       0
  InFragDrops:                    0
  InFragTimeouts:                 0
  OutFragFails:                   0
  InUnknownProtos:                0
  InDelivers:                     159
  OutRequests:                    1012
  OutForwDatagrams:               35
  InNoRoutes:                     0
  InTooBigErrors:                 0
  OutFragOKs:                     0
  OutFragCreates:                 0
  InMcastPkts:                    79
  InMcastNotMembers:              65
  OutMcastPkts:                   938
  InAddrErrors:                   0
  InDiscards:                     0
  OutDiscards:                    0
```

# Display the IPv6 interface settings on Switch B.

```
[SwitchB-Vlan-interface2] display ipv6 interface vlan-interface 2 verbose
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1234
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:0
    FF02::1:FF00:2
    FF02::1:FF00:1234
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                     117
  InTooShorts:                    0
  InTruncatedPkts:                0
  InHopLimitExceeds:              0
  InBadHeaders:                   0
  InBadOptions:                   0
  ReasmReqds:                     0
  ReasmOKs:                       0
  InFragDrops:                    0
  InFragTimeouts:                 0
```

```
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   117
  OutRequests:                  83
  OutForwDatagrams:             0
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  28
  InMcastNotMembers:            0
  OutMcastPkts:                 7
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
```

# Ping Switch A and Switch B on Host, and ping Switch A and Host on Switch B to verify the connectivity between them.

---

**Caution**

When you ping a link-local address, you should use the “–i” parameter to specify an interface for the link-local address.

---

```
[SwitchB-Vlan-interface2] ping ipv6 -c 1 3001::1
  PING 3001::1 : 56  data bytes, press CTRL_C to break
    Reply from 3001::1
    bytes=56 Sequence=1 hop limit=64  time = 2 ms

  --- 3001::1 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
[SwitchB-Vlan-interface2] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
  PING 2001::15B:E0EA:3524:E791 : 56  data bytes, press CTRL_C to break
    Reply from 2001::15B:E0EA:3524:E791
    bytes=56 Sequence=1 hop limit=63  time = 3 ms

  --- 2001::15B:E0EA:3524:E791 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
```

As shown in the output information, Host can ping Switch B and Switch A.

# Troubleshooting IPv6 Basics Configuration

## Symptom

The peer IPv6 address cannot be pinged.

## Solution

- Use the **display current-configuration** command in any view or the **display this** command in system view to verify that IPv6 is enabled.
- Use the **display ipv6 interface** command in any view to verify that the IPv6 address of the interface is correct and the interface is up.
- Use the **debugging ipv6 packet** command in user view to enable the debugging for IPv6 packets to help locate the cause.

# Table of Contents

# 1 Dual Stack Configuration

When configuring dual stack, go to these sections for information you are interested in:

- Dual Stack Overview
- Configuring Dual Stack

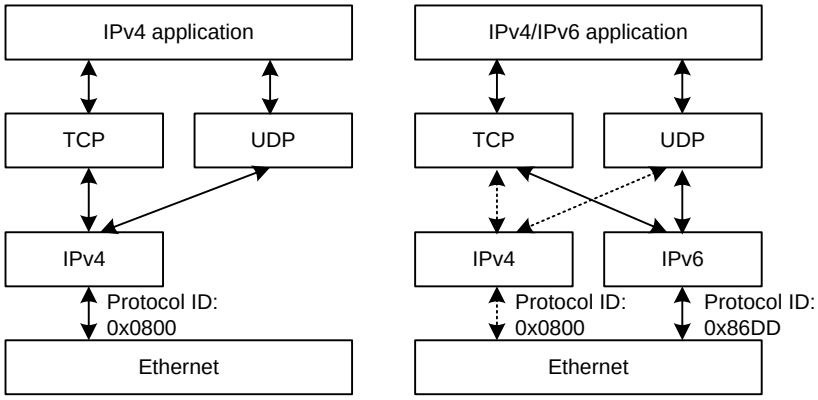
## Dual Stack Overview

Dual stack is the most direct approach to making IPv6 nodes compatible with IPv4 nodes. The best way for an IPv6 node to be compatible with an IPv4 node is to maintain a complete IPv4 stack. A network node that supports both IPv4 and IPv6 is called a dual stack node. A dual stack node configured with an IPv4 address and an IPv6 address can have both IPv4 and IPv6 packets transmitted.

For an upper layer application supporting both IPv4 and IPv6, either TCP or UDP can be selected at the transport layer, while IPv6 stack is preferred at the network layer.

Figure 1-1 illustrates the IPv4/IPv6 dual stack in relation to the IPv4 stack.

**Figure 1-1** IPv4/IPv6 dual stack in relation to IPv4 stack (on Ethernet)




## Configuring Dual Stack

You must enable the IPv6 packet forwarding function before dual stack. Otherwise, the device cannot forward IPv6 packets even if IPv6 addresses are configured for interfaces.

Follow these steps to configure dual stack on a gateway:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the IPv6 packet forwarding function | **ipv6** | Required<br>Disabled by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | | | Use the command… | Remarks |
|---|---|---|---|---|
| Configure an IPv4 address for the interface | | | **ip address** *ip-address* { *mask* \| *mask-length* } [ **sub** ] | Required<br>By default, no IP address is configured. |
| Configure an IPv6 address on the interface | Configure an IPv6 global unicast address or site-local address | Manually specify an IPv6 address | **ipv6 address** { *ipv6-address prefix-length* \| *ipv6-address/prefix-length* } | Use either command.<br>By default, no site-local address or global unicast address is configured on an interface. |
| | | Configure an IPv6 address in the EUI-64 format | **ipv6 address** *ipv6-address/prefix-length* **eui-64** | |
| | Configure an IPv6 link-local address | Automatically create an IPv6 link-local address | **ipv6 address auto link-local** | Optional<br>By default, after you configured an IPv6 site-local address or global unicast address, a link local address is automatically created. |
| | | Manually specify an IPv6 link-local address | **ipv6 address** *ipv6-address* **link-local** | |

**Note**

- For information about IPv4 addressing, refer to *IP Addressing Configuration* in the *IP Services Volume*.
- For more information about IPv6 address, refer to *IPv6 Basics Configuration* in the *IP Services Volume*.
- For how to enable IPv6 and configure an IPv6 address on an interface, refer to *IPv6 Basics Commands* in the *IP Services Volume*.

# Table of Contents

# 1 sFlow Configuration

When configuring sFlow, go to these sections for information you are interested in:



## sFlow Overview

### Introduction to sFlow

Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics.

The sFlow system involves an sFlow agent embedded in a device and a remote sFlow collector. The sFlow agent collects traffic statistics and packets from the sFlow enabled ports on the device, encapsulates the information into sFlow packets, and sends the packets to the sFlow collector. The sFlow collector analyzes the sFlow packets and displays the results.

sFlow has the following two sampling mechanisms:

- Packet-based sampling: An sFlow enabled port samples one packet out of a configurable number of packets passing through it.
- Time-based sampling: The sFlow agent samples the statistics of all sFlow enabled ports at a configurable interval.

As a traffic monitoring technology, sFlow has the following advantages:

- Supporting traffic monitoring on Gigabit and higher-speed networks.
- Providing scalability to allow one sFlow collector to monitor multiple or more sFlow agents.
- Implementing the low-cost sFlow agent.

**Note**

Currently, only the sFlow agent function is supported on 3Com Switch 4500G.

### Operation of sFlow

sFlow operates as follows:

1) With sFlow enabled, a physical port encapsulates sampled data into packets and sends them to the sFlow agent.
2) The sFlow agent periodically collects the statistics of all sFlow enabled ports.

3) When the sFlow packet buffer overflows or the one-second timer expires, the sFlow agent sends sFlow packets to the specified sFlow collector.

## Configuring sFlow

The sFlow feature enables the remote sFlow collector to monitor the network and analyze sFlow packet statistics.

Follow these steps to configure sFlow:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify the IP address of the sFlow agent | **sflow agent ip** *ip-address* | Required<br>Not configured by default. |
| Specify the IP address and port number of the sFlow collector | **sflow collector ip** *ip-address* [ **port** *port-num* ] | Required<br>Not specified by default. |
| Set the counter sampling interval at which the sFlow agent collects the statistics of sFlow enabled ports | **sflow interval** *interval-time* | Optional<br>20 seconds by default. |
| Specify the sFlow version | **sflow version** { **4 \| 5** } | Optional<br>5 by default. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable sFlow in the inbound or outbound direction | **sflow enable** { **inbound** \| **outbound** } | Required<br>Not enabled by default. |
| Specify the sFlow sampling mode | **sflow sampling-mode** { **determine** \| **random** } | Optional<br>**random** by default.<br>Currently, the **determine** mode is not supported on 3Com Switch 4500G. |
| Specify the number of packets out of which the port will sample a packet | **sflow sampling-rate** *rate* | Optional<br>200000 by default. |

**Caution**

- The sFlow agent and sFlow collector must not have the same IP address.
- Currently, you can specify at most two sFlow collectors on 3Com Switch 4500G.

## Displaying and Maintaining sFlow

| To do… | Use the command… | Remarks |
|---|---|---|
| Display sFlow configuration information | **display sflow** | Available in any view |

# sFlow Configuration Example

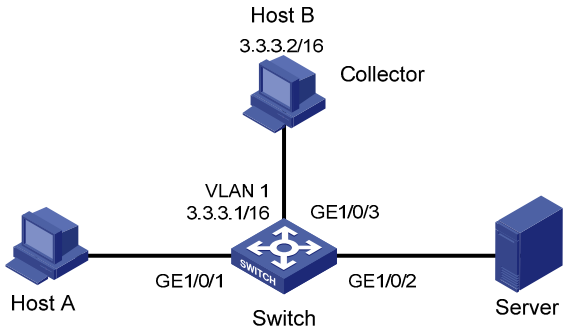
## Network requirements

- Host A and Server are connected to Switch through GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively.
- Host B works as an sFlow collector with IP address 3.3.3.2 and port number 6343, and is connected to Switch through GigabitEthernet 1/0/3.
- GigabitEthernet 1/0/3 belongs to VLAN 1, having an IP address of 3.3.3.1.

Run sFlow agent on Switch, and enable sFlow on GigabitEthernet 1/0/1 to monitor traffic on this port. Switch sends sFlow packets through GigabitEthernet 1/0/3 to Host B, which then analyzes the sFlow packets and displays the results.

## Network diagram

**Figure 1-1** Network diagram for sFlow configuration




## Configuration procedure

# Configure an IP address for the sFlow agent.

```
<Switch> system-view
[Switch] sflow agent ip 3.3.3.1
```

# Specify the IP address and port number of the sFlow collector.

```
[Switch] sflow collector ip 3.3.3.2
```

# Set the sFlow interval to 30 seconds.

```
[Switch] sflow interval 30
```

# Enable sFlow in both the inbound and outbound directions on GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] sflow enable inbound
[Switch-GigabitEthernet1/0/1] sflow enable outbound
```

# Specify the traffic sampling rate.

```
[Switch-GigabitEthernet1/0/1] sflow sampling-rate 100000
```

# Display the sFlow configuration information.

```
[Switch-GigabitEthernet1/0/1] display sflow
sFlow Version: 5
sFlow Global Information:
Agent                   IP:3.3.3.1
```

```
Collector               IP:3.3.3.2  Port:6343
Interval(s): 30
sFlow Port Information:
Interface    Direction       Rate         Mode      Status
GE1/0/1       In/Out          100000       Random    Active
```

# Troubleshooting sFlow Configuration

## The Remote sFlow Collector Cannot Receive sFlow Packets

### Symptom

The remote sFlow collector cannot receive sFlow packets.

### Analysis

- sFlow is not enabled globally because the sFlow agent or/and the sFlow collector is/are not specified.
- No port is enabled with sFlow to sample data.
- The IP address of the sFlow collector specified on the sFlow agent is different from that of the remote sFlow collector.
- No IP address is configured for the Layer 3 interface on the device, or the IP address is configured, but the UDP packets with the IP address being the source cannot reach the sFlow collector.
- The physical link between the device and the sFlow collector fails.

### Solution

1) Check whether sFlow is correctly configured by displaying sFlow configuration with the **display sflow** command.
2) Check whether the correct IP address is configured for the device to communicate with the sFlow collector.
3) Check whether the physical link between the device and the sFlow collector is normal.

# IP Routing Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The IP Routing Volume is organized as follows:

| Features | Description |
|---|---|
| IP Routing Overview | This document describes:<br>• Introduction to IP routing and routing table<br>• Routing protocol overview |
| Static Routing | A static route is manually configured by the administrator. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications. This document describes:<br>• Static route configuration<br>• Detecting Reachability of the Static Route's Nexthop |
| RIP | Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks. This document describes:<br>• RIP basic functions configuration<br>• RIP advanced functions configuration<br>• RIP network optimization configuration |
| IPv6 Static Routing | Static routes are special routes that are manually configured by network administrators. Similar to IPv4 static routes, IPv6 static routes work well in simple IPv6 network environments. This document describes:<br>• IPv6 static route configuration |
| IPv6 RIPng | RIP next generation (RIPng) is an extension of RIP-2 for IPv4. RIPng for IPv6 is IPv6 RIPng. This document describes:<br>• Configuring RIPng Basic Functions<br>• Configuring RIPng Route Control<br>• Tuning and Optimizing the RIPng Network |
| Routing Policy | Routing policy is used on the router for route inspection, filtering, attributes modifying when routes are received, advertised, or redistributed. This document describes:<br>• Defining Filters<br>• Route policy configuration |

# Table of Contents

# 1 IP Routing Overview

Go to these sections for information you are interested in:



**Note**

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

## IP Routing and Routing Table

### Routing

Routing in the Internet is achieved through routers. Upon receiving a packet, a router finds an optimal route based on the destination address and forwards the packet to the next router in the path until the packet reaches the last router, which forwards the packet to the intended destination host.

### Routing Table

#### Routing table

Routing tables play a key role in routing. Each router maintains a routing table, and each entry in the table specifies which physical interface a packet destined for a certain destination should go out to reach the next hop (the next router) or the directly connected destination.

Routes in a routing table can be divided into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

#### Contents of a routing table

A routing table includes the following key items:

- Destination address: Destination IP address or destination network.
- Network mask: Specifies, in company with the destination address, the address of the destination network. A logical AND operation between the destination address and the network mask yields the address of the destination network. For example, if the destination address is 129.102.8.10 and the mask 255.255.0.0, the address of the destination network is 129.102.0.0. A network mask is made of a certain number of consecutive 1s. It can be expressed in dotted decimal format or by the number of the 1s.
- Outbound interface: Specifies the interface through which the IP packets are to be forwarded.

- IP address of the next hop: Specifies the address of the next router on the path. If only the outbound interface is configured, its address will be the IP address of the next hop.
- Priority for the route. Routes to the same destination but having different nexthops may have different priorities and be found by various routing protocols or manually configured. The optimal route is the one with the highest priority (with the smallest metric).

Routes can be divided into two categories by destination:

- Subnet routes: The destination is a subnet.
- Host routes: The destination is a host.

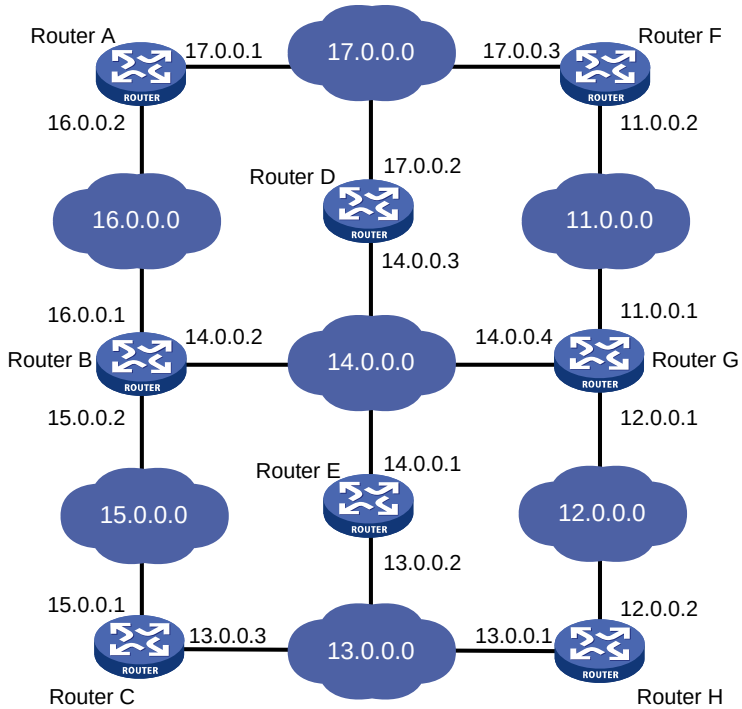
Based on whether the destination is directly connected to a given router, routes can be divided into:

- Direct routes: The destination is directly connected to the router.
- Indirect routes: The destination is not directly connected to the router.

To prevent the routing table from getting too large, you can configure a default route. All packets without matching any entry in the routing table will be forwarded through the default route.

In Figure 1-1, the IP address on each cloud represents the address of the network. Router G is connected to three networks and therefore has three IP addresses for its three physical interfaces. Its routing table is shown under the network topology.

**Figure 1-1** A sample routing table




| Destination Network | Nexthop | Interface |
|---|---|---|
| 11.0.0.0 | 11.0.0.1 | 2 |
| 12.0.0.0 | 12.0.0.1 | 1 |
| 13.0.0.0 | 12.0.0.2 | 1 |
| 14.0.0.0 | 14.0.0.4 | 3 |
| 15.0.0.0 | 14.0.0.2 | 3 |
| 16.0.0.0 | 14.0.0.2 | 3 |
| 17.0.0.0 | 11.0.0.2 | 2 |

# Routing Protocol Overview

## Static Routing and Dynamic Routing

Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. Its major drawback is that you must perform routing configuration again whenever the network topology changes; it cannot adjust to network changes by itself.

Dynamic routing is based on dynamic routing protocols, which can detect network topology changes and recalculate the routes accordingly. Therefore, dynamic routing is suitable for large networks. Its disadvantages are that it is difficult to configure, and that it not only imposes higher requirements on the system, but also consumes a certain amount of network resources.

## Routing Protocols and Routing Priority

Different routing protocols may find different routes to the same destination. However, not all of those routes are optimal. In fact, at a particular moment, only one protocol can uniquely determine the current optimal route to the destination. For the purpose of route selection, each routing protocol (including static routes) is assigned a priority. The route found by the routing protocol with the highest priority is preferred.

The following table lists some routing protocols and the default priorities for routes found by them:

| Routing approach | Priority |
|---|---|
| DIRECT | 0 |
| STATIC | 60 |
| RIP | 100 |
| UNKNOWN | 256 |

**Note**

- The smaller the priority value, the higher the priority.
- The priority for a direct route is always 0, which you cannot change. Any other type of routes can have their priorities manually configured.
- Each static route can be configured with a different priority.
- IPv4 and IPv6 routes have their own respective routing tables.

# Displaying and Maintaining a Routing Table

| To do… | Use the command… | Remarks |
|---|---|---|
| Display brief information about the active routes in the routing table | **display ip routing-table** [ **verbose** \| **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | Available in any view |
| Display information about routes to the specified destination | **display ip routing-table** *ip-address* [ *mask-length* \| *mask* ] [ **longer-match** ] [ **verbose** ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about routes with destination addresses in the specified range | **display ip routing-table** *ip-address1* { *mask-length* \| *mask* } *ip-address2* { *mask-length* \| *mask* } [ **verbose** ] | Available in any view |
| Display information about routes permitted by an IPv4 basic ACL | **display ip routing-table acl** *acl-number* [ **verbose** ] | Available in any view |
| Display routing information permitted by an IPv4 prefix list | **display ip routing-table ip-prefix** *ip-prefix-name* [ **verbose** ] | Available in any view |
| Display routes of a routing protocol | **display ip routing-table protocol** *protocol* [ **inactive** \| **verbose** ] | Available in any view |
| Display statistics about the network routing table | **display ip routing-table statistics** | Available in any view |
| Clear statistics for the routing table | **reset ip routing-table statistics protocol** { **all** \| *protocol* } | Available in user view |
| Display brief IPv6 routing table information | **display ipv6 routing-table** | Available in any view |
| Display verbose IPv6 routing table information | **display ipv6 routing-table verbose** | Available in any view |
| Display routing information for a specified destination IPv6 address | **display ipv6 routing-table** *ipv6-address prefix-length* [ **longer-match** ] [ **verbose** ] | Available in any view |
| Display routing information permitted by an IPv6 ACL | **display ipv6 routing-table acl** *acl6-number* [ **verbose** ] | Available in any view |
| Display routing information permitted by an IPv6 prefix list | **display ipv6 routing-table ipv6-prefix** *ipv6-prefix-name* [ **verbose** ] | Available in any view |
| Display IPv6 routing information of a routing protocol | **display ipv6 routing-table protocol** *protocol* [ **inactive** \| **verbose** ] | Available in any view |
| Display IPv6 routing statistics | **display ipv6 routing-table statistics** | Available in any view |
| Display IPv6 routing information for an IPv6 address range | **display ipv6 routing-table** *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [ **verbose** ] | Available in any view |
| Clear specified IPv6 routing table statistics | **reset ipv6 routing-table statistics protocol** { **all** \| *protocol* } | Available in user view |

# Table of Contents

# 1 Static Routing Configuration

When configuring a static route, go to these sections for information you are interested in:



**Note**

The term "router" in this document refers to a router in a generic sense or a Layer 3 switch.

## Introduction

### Static Route

A static route is a manually configured. If a network's topology is simple, you only need to configure static routes for the network to work normally. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the routes will be unreachable and the network breaks. In this case, the network administrator has to modify the static routes manually.

### Default Route

If the destination address of a packet fails to match any entry in the routing table, the packet will be discarded.

After a default route is configured on a router, any packet whose destination IP address matches no entry in the routing table can be forwarded to a designated upstream router.

A router selects the default route only when it cannot find any matching entry in the routing table.

- If the destination address of a packet fails to match any entry in the routing table, the router selects the default route to forward the packet.
- If there is no default route and the destination address of the packet fails to match any entry in the routing table, the packet will be discarded and an ICMP packet will be sent to the source to report that the destination or the network is unreachable.

Default routes can be configured in two ways:

- The network administrator can configure a default route with both destination and mask being 0.0.0.0. The router forwards any packet whose destination address fails to match any entry in the routing table to the next hop of the default static route.
- Some dynamic routing protocols, such as RIP.

### Application Environment of Static Routing

Before configuring a static route, you need to know the following concepts:

1) Destination address and mask

In the **ip route-static** command, an IPv4 address is in dotted decimal format and a mask can be either in dotted decimal format or in the form of mask length (the digits of consecutive 1s in the mask).

2) Output interface and next hop address

While configuring a static route, you can specify either the output interface or the next hop address depending on the specific occasion. For a NULL0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address

In fact, all the route entries must have a next hop address. When forwarding a packet, a router first searches the routing table for the route to the destination address of the packet. The system can find the corresponding link layer address and forward the packet only after the next hop address is specified. The next hop address can not be a local interface IP address; otherwise, the route configuration will not take effect.

3) Other attributes

You can configure different preferences for different static routes so that route management policies can be applied more flexibly.

## Configuring a Static Route

### Configuration Prerequisites

Before configuring a static route, you need to finish the following tasks:

- Configure the physical parameters for related interfaces
- Configure the link-layer attributes for related interfaces
- Configure the IP addresses for related interfaces

### Configuration Procedure

Follow these steps to configure a static route:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a static route | **ip route-static** *dest-address* { *mask* \| *mask-length* } { *next-hop-address* **\|** *interface-type interface-number next-hop-address* } [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ *description description-text* ] | Required<br>By default, **preference** for static routes is 60, **tag** is 0, and no description information is configured. |
| Configure the default preference for static routes | **ip route-static default-preference** *default-preference-value* | Optional<br>60 by default |

**Note**

- When configuring a static route, the static route does not take effect if you specify the next hop address first and then configure it as the IP address of a local interface.
- If you do not specify the preference when configuring a static route, the default preference will be used. Reconfiguring the default preference applies only to newly created static routes.
- You can flexibly control static routes by configuring tag values and using the tag values in the routing policy.
- If the destination IP address and mask are both configured as 0.0.0.0 with the **ip route-static** command, the route is the default route.

## Detecting Reachability of the Static Route's Nexthop

If a static route fails due to a topology change or a fault, the connection will be interrupted. To improve network stability, the system needs to detect reachability of the static route's next hop and switch to a backup route once the next hop is unreachable.

Following method can be used to detect reachability of the static route's next hop.

### Detecting Nexthop Reachability Through Track

If you specify the nexthop but not outgoing interface when configuring a static route, you can associate the static route with a track entry to check the static route validity:

- When the track entry is positive, the static route's nexthop is reachable and the static route takes effect.
- When the track entry is negative, the static route's nexthop is unreachable and the static route is invalid. For details about track, refer to *Track Configuration* in the *System Volume*.

### Network requirements

To detect the reachability of a static route's nexthop through a Track entry, you need to create a Track first. For detailed Track configuration procedure, refer to *Track Configuration* in the *System Volume*.

### Configuration procedure

Follow these steps to detect the reachability of a static route's nexthop through Track:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Associate the static route with a track entry | **ip route-static** *dest-address* { *mask* **|** *mask-length* } *next-hop-address* **track** *track-entry-number* [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **description** *description-text* ] | Required<br>Not configured by default |

**Note**

- To configure this feature for an existing static route, simply associate the static route with a track entry. For a non-existent static route, configure it and associate it with a Track entry.
- If a static route needs route recursion, the associated track entry must monitor the nexthop of the recursive route instead of that of the static route; otherwise, a valid route may be mistakenly considered invalid.

## Displaying and Maintaining Static Routes

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current configuration information | **display current-configuration** | Available in any view |
| Display the brief information of the IP routing table | **display ip routing-table** | |
| Display the detailed information of the IP routing table | **display ip routing-table verbose** | |
| View information of static routes | **display ip routing-table protocol static** [ **inactive** | **verbose** ] | |
| Delete all the static routes | **delete static-routes all** | Available In system view |

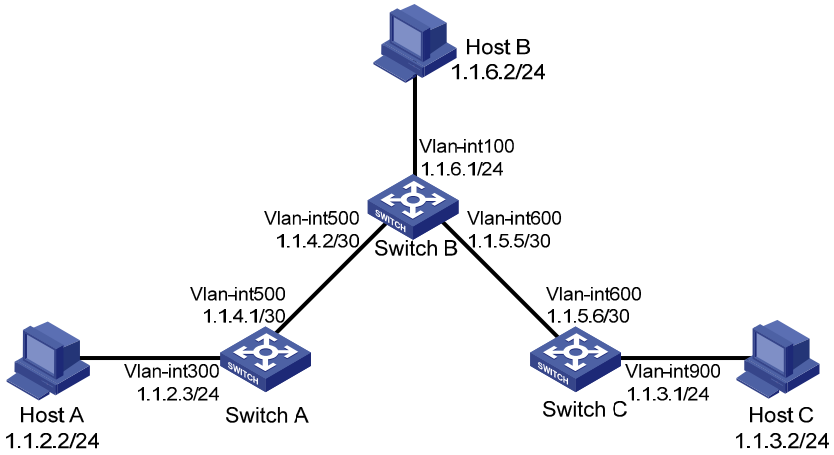
## Static Route Configuration Example

### Basic Static Route Configuration Example

#### Network requirements

The IP addresses and masks of the switches and hosts are shown in the following figure. Static routes are required for interconnection between any two hosts.

**Figure 1-1** Network diagram for static route configuration




## Configuration procedure

1) Configuring IP addresses for interfaces (omitted)
2) Configuring static routes

# Configure a default route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

# Configure two static routes on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

# Configure a default route on Switch C

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

3) Configure the hosts.

The default gateways for the three hosts A, B and C are 1.1.2.3, 1.1.6.1 and 1.1.3.1 respectively. The configuration procedure is omitted.

4) Display the configuration.

# Display the IP routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 7       Routes : 7

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            1.1.4.2         Vlan500
1.1.2.0/24          Direct 0    0            1.1.2.3         Vlan300
1.1.2.3/32          Direct 0    0            127.0.0.1       InLoop0
1.1.4.0/30          Direct 0    0            1.1.4.1         Vlan500
1.1.4.1/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

# Display the IP routing table of Switch B.

```
[SwitchB] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.2.0/24          Static 60   0            1.1.4.1         Vlan500
1.1.3.0/24          Static 60   0            1.1.5.6         Vlan600
1.1.4.0/30          Direct 0    0            1.1.4.2         Vlan500
1.1.4.2/32          Direct 0    0            127.0.0.1       InLoop0
1.1.5.4/30          Direct 0    0            1.1.5.5         Vlan600
1.1.5.5/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
1.1.6.0/24          Direct 0    0            192.168.1.47    Vlan100
1.1.6.1/32          Direct 0    0            127.0.0.1       InLoop0
```

# Use the **ping** command on Host B to check reachability to Host A, assuming Windows XP runs on the two hosts.

```
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=255
Reply from 1.1.2.2: bytes=32 time=1ms TTL=255
Reply from 1.1.2.2: bytes=32 time=1ms TTL=255
Reply from 1.1.2.2: bytes=32 time=1ms TTL=255

Ping statistics for 1.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

# Use the **tracert** command on Host B to check reachability to Host A.

```
[HostB] tracert 1.1.2.2

Tracing route to 1.1.2.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  1.1.6.1
  2    <1 ms    <1 ms    <1 ms  1.1.4.1
  3     1 ms    <1 ms    <1 ms  1.1.2.2

Trace complete.
```

# Table of Contents

# 1 RIP Configuration

**Note**

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

When configuring RIP, go to these sections for information you are interested in:



## RIP Overview

RIP is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks, such as academic networks and simple LANs. RIP is not applicable to complex networks.

RIP is still widely used in practical networking due to easier implementation, configuration and maintenance than OSPF and IS-IS.

### Operation of RIP

#### Introduction

RIP is a distance vector routing protocol, using UDP packets for exchanging information through port 520.

RIP uses a hop count to measure the distance to a destination. The hop count from a router to a directly connected network is 0. The hop count from a router to a directly connected router is 1. To limit convergence time, the range of RIP metric value is from 0 to 15. A metric value of 16 (or greater) is considered infinite, which means the destination network is unreachable. That is why RIP is not suitable for large-scaled networks.

RIP prevents routing loops by implementing the split horizon and poison reverse functions.

#### RIP routing table

A RIP router has a routing table containing routing entries of all reachable destinations, and each routing entry contains:

- Destination address: IP address of a host or a network.
- Next hop: IP address of the adjacent router’s interface to reach the destination.

- Egress interface: Packet outgoing interface.
- Metric: Cost from the local router to the destination.
- Route time: Time elapsed since the routing entry was last updated. The time is reset to 0 every time the routing entry is updated.
- Route tag: Identifies a route, used in a routing policy to flexibly control routes. For information about routing policy, refer to *Routing Policy Configuration* in the *IP Routing Volume*.

### RIP timers

RIP employs four timers, update, timeout, suppress, and garbage-collect.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no update for a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the garbage-collect timer expires, the route will be deleted from the routing table.

### Routing loops prevention

RIP is a distance vector (D-V) routing protocol. Since a RIP router advertises its own routing table to neighbors, routing loops may occur.

RIP uses the following mechanisms to prevent routing loops.

- Counting to infinity. The metric value of 16 is defined as unreachable. When a routing loop occurs, the metric value of the route will increment to 16.
- Split horizon. A router does not send the routing information learned from a neighbor to the neighbor to prevent routing loops and save bandwidth.
- Poison reverse. A router sets the metric of routes received from a neighbor to 16 and sends back these routes to the neighbor to help delete such information from the neighbor's routing table.
- Triggered updates. A router advertises updates once the metric of a route is changed rather than after the update period expires to speed up network convergence.

## Operation of RIP

The following procedure describes how RIP works.

1) After RIP is enabled, the router sends request messages to neighboring routers. Neighboring routers return Response messages including information about their routing tables.
2) After receiving such information, the router updates its local routing table, and sends triggered update messages to its neighbors. All routers on the network do the same to keep the latest routing information.
3) By default, a RIP router sends its routing table to neighbors every 30 seconds.
4) RIP ages out routes by adopting an aging mechanism to keep only valid routes.

## RIP Version

RIP has two versions, RIPv1 and RIPv2.

RIPv1, a classful routing protocol, supports message advertisement via broadcast only. RIPv1 protocol messages do not carry mask information, which means it can only recognize routing information of natural networks such as Class A, B, C. That is why RIPv1 does not support discontiguous subnets.

RIPv2 is a classless routing protocol. Compared with RIPv1, RIPv2 has the following advantages.

- Supporting route tags. Route tags are used in routing policies to flexibly control routes.
- Supporting masks, route summarization and Classless Inter-Domain Routing (CIDR).
- Supporting designated next hops to select the best next hops on broadcast networks.
- Supporting multicast routing update to reduce resource consumption.
- Supporting plain text authentication and MD5 authentication to enhance security.

---

**Note**

RIPv2 has two types of message transmission: broadcast and multicast. Multicast is the default type using 224.0.0.9 as the multicast address. The interface working in the RIPv2 broadcast mode can also receive RIPv1 messages.

---

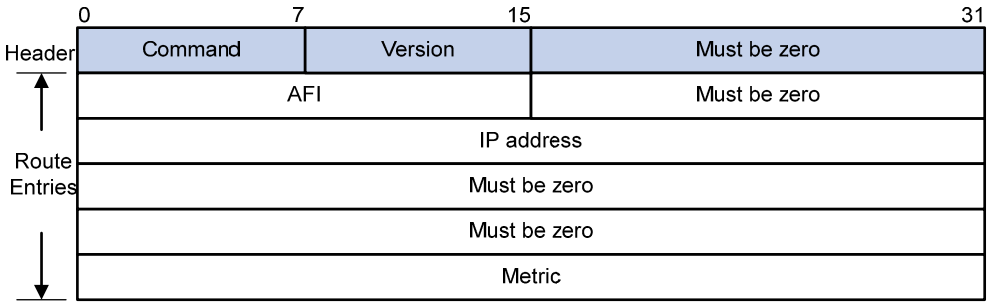
## RIP Message Format

A RIPv1 message consists of a header and up to 25 route entries. (A RIPv2 authentication message uses the first route entry as the authentication entry, so it has up to 24 route entries.)

### RIPv1 message format

Figure 1-1 shows the format of RIPv1 message.

**Figure 1-1** RIPv1 Message Format

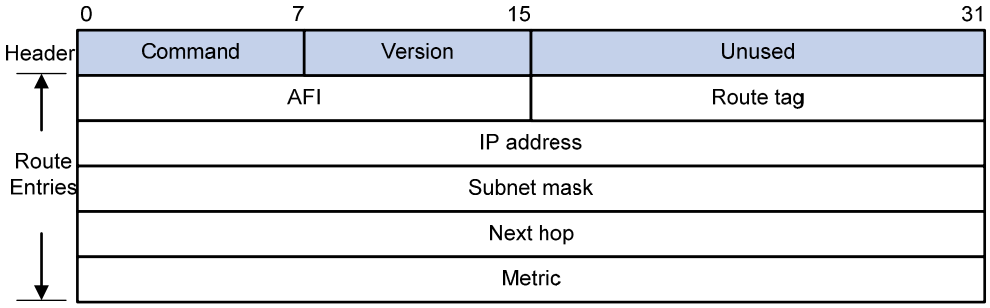



- Command: Type of message. 1 indicates request, which is used to request all or part of the routing information from the neighbor, and 2 indicates response, which contains all or part of the routing information. A response message consists of up to 25 route entries.
- Version: Version of RIP, 0x01 for RIPv1.
- Must be zero: This field must be zero.
- AFI: Address Family Identifier, 2 for IP, and 0 for request messages.
- IP Address: Destination IP address of the route. It can be a natural network, subnet or a host address.
- Metric: Cost of the route, 16 for request messages.

## RIPv2 message format

The format of RIPv2 message is similar to RIPv1. Figure 1-2 shows it.

**Figure 1-2** RIPv2 Message Format



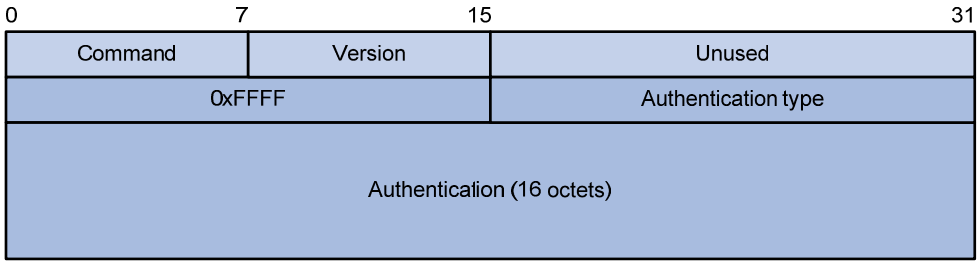

The differences from RIPv1 are stated as following.

- Version: Version of RIP. For RIPv2 the value is 0x02.
- Route Tag: Route Tag.
- IP Address: Destination IP address. It can be a natural network address, subnet address or host address.
- Subnet Mask: Mask of the destination address.
- Next Hop: If set to 0.0.0.0, it indicates that the originator of the route is the best next hop; otherwise it indicates a next hop better than the originator of the route.

## RIPv2 authentication

RIPv2 sets the AFI field of the first route entry to 0xFFFF to identify authentication information. See Figure 1-3.

**Figure 1-3** RIPv2 Authentication Message




- Authentication Type: A value of 2 represents plain text authentication, while a value of 3 represents MD5.
- Authentication: Authentication data, including password information when plain text authentication is adopted or including key ID, MD5 authentication data length and sequence number when MD5 authentication is adopted.

**Note**

- RFC 1723 only defines plain text authentication. For information about MD5 authentication, refer to RFC 2453 “RIP Version 2”.
- With RIPv1, you can configure the authentication mode in interface view. However, the configuration will not take effect because RIPv1 does not support authentication.

## Supported RIP Features

The current implementation supports the following RIP features.

- RIPv1 and RIPv2
- RIP multi-instance.

## Protocols and Standards

- RFC 1058: Routing Information Protocol
- RFC 1723: RIP Version 2 - Carrying Additional Information
- RFC 1721: RIP Version 2 Protocol Analysis
- RFC 1722: RIP Version 2 Protocol Applicability Statement
- RFC 1724: RIP Version 2 MIB Extension
- RFC 2082: RIPv2 MD5 Authentication
- RFC2453: RIP Version 2

# Configuring RIP Basic Functions

## Configuration Prerequisites

Before configuring RIP basic functions, complete the following tasks.

- Configure the link layer protocol.
- Configure an IP address on each interface, and make sure all adjacent routers are reachable to each other.

## Configuration Procedure

### Enabling RIP and a RIP interface

Follow these steps to enable RIP:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable a RIP process and enter RIP view | **rip** [ *process-id* ] | Required<br>Not enabled by default |
| Enable RIP on the interface attached to the specified network | **network** *network-address* | Required<br>Disabled by default |

**Note**

- If you make some RIP configurations in interface view before enabling RIP, those configurations will take effect after RIP is enabled.
- RIP runs only on the interfaces residing on the specified networks. Therefore, you need to specify the network after enabling RIP to validate RIP on a specific interface.
- You can enable RIP on all interfaces using the command **network** 0.0.0.0.

### Configuring the interface behavior

Follow these steps to configure the interface behavior:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Disable an or all interfaces from sending routing updates (the interfaces can still receive updates) | **silent-interface** { *interface-type interface-number* \| **all** } | Optional<br>All interfaces can send routing updates by default. |
| Return to system view | **quit** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the interface to receive RIP messages | **rip input** | Optional<br>Enabled by default |
| Enable the interface to send RIP messages | **rip output** | Optional<br>Enabled by default |

### Configuring a RIP version

You can configure a RIP version in RIP or interface view.

- If neither global nor interface RIP version is configured, the interface sends RIPv1 broadcasts and can receive RIPv1 broadcast and unicast packets, and RIPv2 broadcast, multicast, and unicast packets.
- If an interface has no RIP version configured, it uses the global RIP version; otherwise it uses the RIP version configured on it.
- With RIPv1 configured, an interface sends RIPv1 broadcasts, and can receive RIPv1 broadcasts and RIPv1 unicasts.
- With RIPv2 configured, a multicast interface sends RIPv2 multicasts and can receive RIPv2 unicasts, broadcasts and multicasts.
- With RIPv2 configured, a broadcast interface sends RIPv2 broadcasts and can receive RIPv1 unicasts, and broadcasts, and RIPv2 broadcasts, multicasts and unicasts.

Follow these steps to configure a RIP version:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Specify a global RIP version | **version** { **1** \| **2** } | Optional<br>By default, if an interface has a RIP version specified, the version takes precedence over the global one. If no RIP version is specified for an interface, the interface can send RIPv1 broadcasts, and receive RIPv1 broadcasts, unicasts, RIPv2 broadcasts, multicasts and unicasts. |
| Return to system view | **quit** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Specify a RIP version for the interface | **rip version** { **1** \| **2** [ **broadcast** \| **multicast** ] } | Optional |

# Configuring RIP Route Control

In complex networks, you need to configure advanced RIP features.

This section covers the following topics:

- Configuring an Additional Routing Metric
- Configuring RIPv2 Route Summarization
- Disabling Host Route Reception
- Advertising a Default Route
- Configuring Inbound/Outbound Route Filtering
- Configuring a Priority for RIP
- Configuring RIP Route Redistribution

Before configuring RIP routing feature, complete the following tasks:

- Configure an IP address for each interface, and make sure all neighboring routers are reachable to each other.
- Configure RIP basic functions

## Configuring an Additional Routing Metric

An additional routing metric can be added to the metric of an inbound or outbound RIP route.

The outbound additional metric is added to the metric of a sent route, and the route's metric in the routing table is not changed.

The inbound additional metric is added to the metric of a received route before the route is added into the routing table, and the route's metric is changed. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

Follow these steps to configure additional routing metrics:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Define an inbound additional routing metric | **rip metricin** [ **route-policy** *route-policy-name* ] *value* | Optional<br>0 by default |
| Define an outbound additional routing metric | **rip metricout** [ **route-policy** *route-policy-name* ] *value* | Optional<br>1 by default |

## Configuring RIPv2 Route Summarization

Route summarization means that subnets in a natural network are summarized into a natural network that is sent to other networks. This feature can reduce the size of routing tables.

### Enabling RIPv2 route automatic summarization

You can disable RIPv2 route automatic summarization if you want to advertise all subnet routes.

Follow these steps to enable RIPv2 route automatic summarization:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Enable RIPv2 automatic route summarization | **summary** | Optional<br>Enabled by default |

### Advertising a summary route

You can configure RIPv2 to advertise a summary route on the specified interface.

To do so, use the following commands:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Disable RIPv2 automatic route summarization | **undo summary** | Required<br>Enabled by default |
| Return to system view | **quit** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Advertise a summary route | **rip summary-address** *ip-address* { *mask* \| *mask-length* } | Required |

**Note**

You need to disable RIPv2 route automatic summarization before advertising a summary route on an interface.

## Disabling Host Route Reception

Sometimes a router may receive from the same network many host routes, which are not helpful for routing and consume a large amount of network resources. In this case, you can disable RIP from receiving host routes to save network resources.

Follow these steps to disable RIP from receiving host routes:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Disable RIP from receiving host routes | **undo host-route** | Required<br>Enabled by default |

**Note**

RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

## Advertising a Default Route

You can configure RIP to advertise a default route with a specified metric to RIP neighbors.

- In RIP view, you can configure all the interfaces of the RIP process to advertise a default route; in interface view, you can configure a RIP interface of the RIP process to advertise a default route. The latter takes precedence over the former on the interface.
- If a RIP process is enabled to advertise a default route, to disable an interface of the RIP process from default route advertisement, you can use the **rip default-route no-originate** command on the interface.

Follow these steps to configure RIP to advertise a default route:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Enable RIP to advertise a default route | **default-route** { **only** \| **originate** } [ **cost** *cost* ] | Optional<br>Not enabled by default |
| Return to system view | **quit** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the RIP interface to advertise a default route | **rip default-route** { { **only** \| **originate** } [ **cost** *cost* ] \| **no-originate** } | Optional<br>By default, a RIP interface can advertise a default route if the RIP process is configured with default route advertisement. |

**Note**

The router enabled to advertise a default route does not receive default routes from RIP neighbors.

## Configuring Inbound/Outbound Route Filtering

The device supports route filtering. You can filter routes by configuring the inbound and outbound route filtering policies by referencing an ACL or IP prefix list. You can also configure the router to receive only routes from a specified neighbor.

Follow these steps to configure route filtering:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Configure the filtering of incoming routes | **filter-policy** { *acl-number* \| **gateway** *ip-prefix-name* \| **ip-prefix** *ip-prefix-name* [ **gateway** *ip-prefix-name* ] } **import** [ *interface-type interface-number* ] | Required<br>Not configured by default |
| Configure the filtering of outgoing routes | **filter-policy** { *acl-number* \| **ip-prefix** *ip-prefix-name* } **export** [ *protocol* [ *process-id* ] \| *interface-type interface-number* ] | Required<br>Not configured by default |

**Note**

- Using the **filter-policy import** command filters incoming routes. Routes not passing the filtering will be neither installed into the routing table nor advertised to neighbors.
- Using the **filter-policy export** command filters outgoing routes, including routes redistributed with the **import-route** command.

## Configuring a Priority for RIP

Multiple IGP protocols may run in a router. If you want RIP routes to have a higher priority than those learned by other routing protocols, you can assign RIP a smaller priority value to influence optimal route selection.

Follow these steps to configure a priority for RIP:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Configure a priority for RIP | **preference** [ **route-policy** *route-policy-name* ] *value* | Optional<br>100 by default |

### Configuring RIP Route Redistribution

If a router runs RIP and other routing protocols, you can configure RIP to redistribute static or direct routes.

Follow these steps to configure RIP route redistribution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Configure a default metric for redistributed routes | **default cost** *value* | Optional<br>The default metric of a redistributed route is 0 by default. |
| Redistribute routes from another protocol | **import-route** *protocol* [ *process-id* \| **all-processes** ] [ **cost** *cost* \| **route-policy** *route-policy-name* \| **tag** *tag* ] * | Required<br>No redistribution is configured by default. |

**Note**

Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.

## Configuring RIP Network Optimization

Complete the following tasks before configuring RIP network optimization:

- Configure network addresses for interfaces, and make neighboring nodes reachable to each other;
- Configure RIP basic functions.

### Configuring RIP Timers

Follow these steps to configure RIP timers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure values for RIP timers | **timers** { **garbage-collect** *garbage-collect-value* \| **suppress** *suppress-value* \| **timeout** *timeout-value* \| **update** *update-value* } * | Optional<br>The default update timer, timeout timer, suppress timer, and garbage-collect timer are 30s, 180s, 120s and 120s respectively. |

**Note**

Based on network performance, you need to make RIP timers of RIP routers identical to each other to avoid unnecessary traffic or route oscillation.

## Configuring Split Horizon and Poison Reverse

**Note**

If both split horizon and poison reverse are configured, only the poison reverse function takes effect.

### Enabling split horizon

The split horizon function disables an interface from sending routes received from the interface to prevent routing loops between adjacent routers.

Follow these steps to enable split horizon:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable split horizon | **rip split-horizon** | Optional<br>Enabled by default |

### Enabling poison reverse

The poison reverse function allows an interface to advertise the routes received from it, but the metric of these routes is set to 16, making them unreachable.

Follow these steps to enable poison reverse:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable poison reverse | **rip poison-reverse** | Required<br>Disabled by default |

## Enabling Zero Field Check on Incoming RIPv1 Messages

Some fields in the RIPv1 message must be zero. These fields are called zero fields. You can enable zero field check on received RIPv1 messages. If such a field contains a non-zero value, the RIPv1 message will not be processed. If you are sure that all messages are trusty, you can disable zero field check to save CPU resources.

This task does not apply to RIPv2 packets that have no zero fields.

Follow these steps to enable zero field check on incoming RIPv1 messages:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Enable zero field check on received RIPv1 messages | **checkzero** | Optional<br>Enabled by default |

## Enabling Source IP Address Check on Incoming RIP Updates

You can enable source IP address check on incoming RIP updates.

For a message received, RIP compares the source IP address of the message with the IP address of the interface. If they are not in the same network segment, RIP discards the message.

Follow these steps to enable source IP address check on incoming RIP updates:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Enable source IP address check on incoming RIP messages | **validate-source-address** | Optional<br>Enabled by default |

**Note**

The source IP address check feature should be disabled if the RIP neighbor is not directly connected.

## Configuring RIPv2 Message Authentication

RIPv2 supports two authentication modes: plain text and MD5.

In plain text authentication, the authentication information is sent with the RIP message, which however cannot meet high security needs.

Follow these steps to configure RIPv2 message authentication:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure RIPv2 authentication | **rip authentication-mode** { **md5** { **rfc2082** *key-string key-id* \| **rfc2453** *key-string* } \| **simple** *password* } | Required |

**Note**

This task does not apply to RIPv1 because RIPv1 does not support authentication. Although you can specify authentication modes for RIPv1 in interface view, the configuration does not take effect.

## Specifying a RIP Neighbor

Usually, RIP sends messages to broadcast or multicast addresses. On non broadcast or multicast links, you need to manually specify RIP neighbors. If a specified neighbor is not directly connected, you must disable source address check on incoming updates.

Follow these steps to specify a RIP neighbor:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIP view | **rip** [ *process-id* ] | — |
| Specify a RIP neighbor | **peer** *ip-address* | Required |
| Disable source address check on incoming RIP updates | **undo validate-source-address** | Required<br>Not disabled by default |

**Note**

- You need not use the **peer** *ip-address* command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.
- If a specified neighbor is not directly connected, you need to disable source address check on incoming updates.

## Configuring RIP-to-MIB Binding

This task allows you to enable a specific RIP process to receive SNMP requests.

Follow these steps to bind RIP to MIB:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Bind RIP to MIB | **rip mib-binding** *process-id* | Optional<br>By default, MIB is bound to RIP process 1. |

### Configuring the RIP Packet Sending Rate

RIP periodically sends routing information in RIP packets to RIP neighbors.

Sending large numbers of RIP packets at the same time may affect device performance and consume large network bandwidth. To solve this problem, you can specify the maximum number of RIP packets that can be sent at the specified interval.

Follow these steps to configure the RIP packet sending rate:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable a RIP process and enter RIP view | **rip** [ *process-id* ] | — |
| Configure the maximum number of RIP packets that can be sent at the specified interval | **output-delay** *time* **count** *count* | Optional<br>By default, an interface sends up to three RIP packets every 20 milliseconds. |

## Displaying and Maintaining RIP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display RIP current status and configuration information | **display rip** [ *process-id* ] | Available in any view |
| Display all active routes in RIP database | **display rip** *process-id* **database** | |
| Display RIP interface information | **display rip** *process-id* **interface** [ *interface-type interface-number* ] | |
| Display routing information about a specified RIP process | **display rip** *process-id* **route** [ *ip-address* { *mask* \| *mask-length* } \| **peer** *ip-address* \| **statistics** ] | |
| Clear the statistics of a RIP process | **reset rip** *process-id* **statistics** | Available in user view |

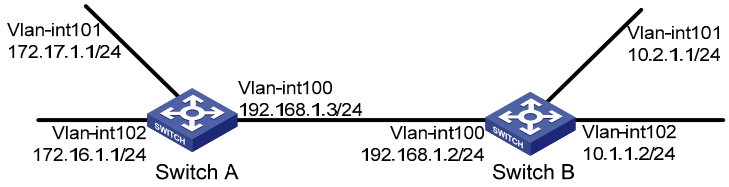
## RIP Configuration Examples

### Configuring RIP Version

#### Network requirements

As shown in Figure 1-4, enable RIPv2 on all interfaces on Switch A and Switch B.

**Figure 1-4** Network diagram for RIP version configuration




## Configuration procedure

1) Configure an IP address for each interface (only the IP address configuration for the VLAN interfaces is given in the following examples)

# Configure Switch A.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.1.3 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ip address 172.17.1.1 24
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ip address 172.16.1.1 24
```

# Configure Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.168.1.2 24
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 10.2.1.1 24
[SwitchB-Vlan-interface101] quit
```

2) Configure basic RIP functions

# Configure Switch A.

```
[SwitchA] rip
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] network 172.16.0.0
[SwitchA-rip-1] network 172.17.0.0
```

# Configure Switch B.

```
[SwitchB] rip
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 10.0.0.0
```

# Display the RIP routing table of Switch A.

```
[SwitchA] display rip 1 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlan-interface100
```

```
      Destination/Mask        Nexthop     Cost    Tag    Flags   Sec
         10.0.0.0/8        192.168.1.2      1       0     RA      11
```

From the routing table, you can find that RIPv1 uses a natural mask.

3) On Switch A and Switch B, specify the RIP version as RIPv2, and disable RIPv2 route automatic summarization to advertise all subnet routes.

# Configure RIPv2 on Switch A.

```
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
```

# Configure RIPv2 on Switch B.

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

# Display the RIP routing table on Switch A.

```
[SwitchA] display rip 1 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 192.168.1.2  on Vlan-interface100
      Destination/Mask        Nexthop     Cost    Tag    Flags   Sec
         10.0.0.0/8        192.168.1.2      1       0     RA      50
         10.2.1.0/24       192.168.1.2      1       0     RA      16
         10.1.1.0/24       192.168.1.2      1       0     RA      16
```

From the routing table, you can see RIPv2 uses classless subnet mask.

---

**Note**

Since the routing information advertised by RIPv1 has a long aging time, it will still exist until it ages out after RIPv2 is configured.

---

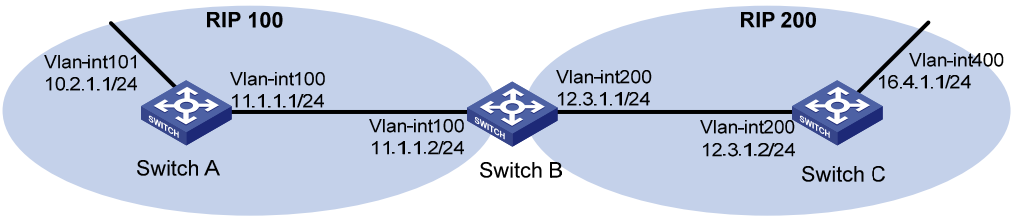
## Configuring RIP Route Redistribution

### Network requirements

As shown in the following figure:

- Two RIP processes are running on Switch B, which communicates with Switch A through RIP 100 and with Switch C through RIP 200.
- Configure route redistribution on Switch B to make RIP 200 redistribute direct routes and routes from RIP 100. Thus, Switch C can learn routes destined for 10.2.1.0/24 and 11.1.1.0/24, while Switch A cannot learn routes destined for 12.3.1.0/24 and 16.4.1.0/24.
- Configure a filtering policy on Switch B to filter out the route 10.2.1.1/24 from RIP 100, making the route not advertised to Switch C.

**Figure 1-5** Network diagram for RIP route redistribution configuration




## Configuration procedure

1) Configure an IP address for each interface (Omitted).
2) Configure basic RIP functions.

# Enable RIP 100 and specify RIP version 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] rip 100
[SwitchA-rip-100] network 10.0.0.0
[SwitchA-rip-100] network 11.0.0.0
[SwitchA-rip-100] version 2
[SwitchA-rip-100] undo summary
[SwitchA-rip-100] quit
```

# Enable RIP 100 and RIP 200 and specify RIP version 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] rip 100
[SwitchB-rip-100] network 11.0.0.0
[SwitchB-rip-100] version 2
[SwitchB-rip-100] undo summary
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 12.0.0.0
[SwitchB-rip-200] version 2
[SwitchB-rip-200] undo summary
[SwitchB-rip-200] quit
```

# Enable RIP 200 and specify RIP version 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] rip 200
[SwitchC-rip-200] network 12.0.0.0
[SwitchC-rip-200] network 16.0.0.0
[SwitchC-rip-200] version 2
[SwitchC-rip-200] undo summary
```

# Display the routing table of Switch C.

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 6        Routes : 6
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
```

```
12.3.1.2/32         Direct 0    0           127.0.0.1       InLoop0
16.4.1.0/24         Direct 0    0           16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
```

3) Configure route redistribution

# On Switch B, configure RIP 200 to redistribute direct routes and routes from RIP 100.

```
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] import-route direct
[SwitchB-rip-200] quit
```

# Display the routing table of Switch C.

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 8        Routes : 8
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         RIP    100  1            12.3.1.1        Vlan200
11.1.1.0/24         RIP    100  1            12.3.1.1        Vlan200
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
16.4.1.0/24         Direct 0    0            16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

4) Configure an filtering policy to filter redistributed routes

# Configure ACL 2000 to filter routes redistributed from RIP 100 on Switch B, making the route 10.2.1.0/24 not advertised to Switch C.

```
[SwitchB] acl number 2000
[SwitchB-acl-basic-2000] rule deny source 10.2.1.1 0.0.0.255
[SwitchB-acl-basic-2000] rule permit
[SwitchB-acl-basic-2000] quit
[SwitchB] rip 200
[SwitchB-rip-200] filter-policy 2000 export rip 100
```

# Display the routing table of Switch C.

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.1.1.0/24         RIP    100  1            12.3.1.1        Vlan200
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
16.4.1.0/24         Direct 0    0            16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

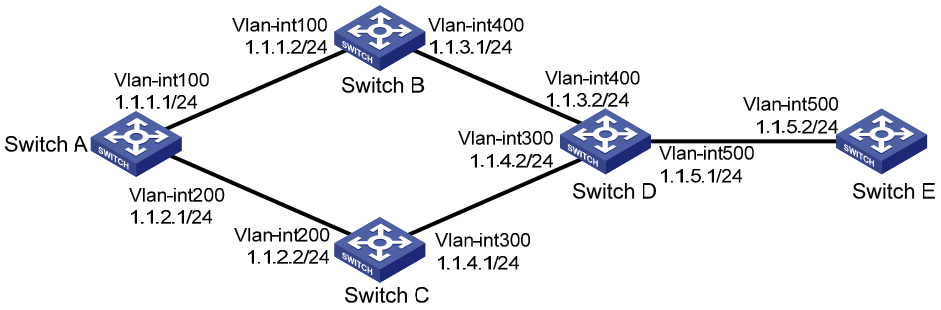
## Configuring an Additional Metric for a RIP Interface

### Network requirements

As shown in the following figure:

- RIP is enabled on all the interfaces of Switch A, Switch B, Switch C, Switch D, and Switch E. The switches are interconnected through RIPv2.
- Switch A has two links to Switch D. The link from Switch B to Switch D is more stable than that from Switch C to Switch D. Configure an additional metric for RIP routes received through VLAN-interface 200 on Switch A so that Switch A prefers the 1.1.5.0/24 network learned from Switch B.

**Figure 1-6** Network diagram for RIP interface additional metric configuration




### Configuration procedure

1) Configure IP addresses for the interfaces (omitted).
2) Configure RIP basic functions.

# Configure Switch A.

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

# Configure Switch B.

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 1.0.0.0
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

# Configure Switch C.

```
<SwitchC> system-view
[SwitchB] rip 1
[SwitchC-rip-1] network 1.0.0.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

# Configure Switch D.

```
<SwitchD> system-view
```

```
[SwitchD] rip 1
[SwitchD-rip-1] network 1.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

# Configure Switch E.

```
<SwitchE> system-view
[SwitchE] rip 1
[SwitchE-rip-1] network 1.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

# Display the IP routing table of Switch A.

```
[SwitchA] display rip 1 database
   1.0.0.0/8, cost 0, ClassfulSumm
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 1, nexthop 1.1.2.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.2.2
```

The display shows that there are two RIP routes to network 1.1.5.0/24. Their next hops are Switch B (1.1.1.2) and Switch C (1.1.2.2) respectively, with the same cost of 2. Switch C is the next hop router to reach network 1.1.4.0/24, with a cost of 1.

3) Configure an additional metric for the RIP interface.

# Configure an additional metric of 3 for VLAN-interface 200 on Switch A.

```
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] rip metricin 3
[SwitchA-Vlan-interface200] display rip 1 database
   1.0.0.0/8, cost 0, ClassfulSumm
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
```

The display shows that there is only one RIP route to network 1.1.5.0/24, with the next hop as Switch B (1.1.1.2) and a cost of 2.

# Troubleshooting RIP

## No RIP Updates Received

**Symptom:**

No RIP updates are received when the links work well.

**Analysis:**

After enabling RIP, you must use the **network** command to enable corresponding interfaces. Make sure no interfaces are disabled from handling RIP messages.

If the peer is configured to send multicast messages, the same should be configured on the local end.

**Solution:**

- Use the **display current-configuration** command to check RIP configuration
- Use the **display rip** command to check whether some interface is disabled

## Route Oscillation Occurred

**Symptom:**

When all links work well, route oscillation occurs on the RIP network. After displaying the routing table, you may find some routes appear and disappear in the routing table intermittently.

**Analysis:**

In the RIP network, make sure all the same timers within the whole network are identical and relationships between timers are reasonable. For example, the timeout timer value should be greater than the update timer value.

**Solution:**

- Use the **display rip** command to check the configuration of RIP timers
- Use the **timers** command to adjust timers properly.

# Table of Contents

# 1 IPv6 Static Routing Configuration

When configuring IPv6 Static Routing, go to these sections for information you are interested in:



**Note**

The term “router” in this document refers to either a router in a generic sense or a Layer 3 switch running routing protocols.

## Introduction to IPv6 Static Routing

Static routes are special routes that are manually configured by network administrators. They work well in simple networks. Configuring and using them properly can improve the performance of networks and guarantee enough bandwidth for important applications.

However, static routes also have shortcomings: any topology changes could result in unavailable routes, requiring the network administrator to manually configure and modify the static routes.

### Features of IPv6 Static Routes

Similar to IPv4 static routes, IPv6 static routes work well in simple IPv6 network environments.

Their major difference lies in the destination and next hop addresses. IPv6 static routes use IPv6 addresses whereas IPv4 static routes use IPv4 addresses.

### Default IPv6 Route

The IPv6 static route that has the destination address configured as **::/0** (indicating a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

## Configuring an IPv6 Static Route

In small IPv6 networks, IPv6 static routes can be used to forward packets. In comparison to dynamic routes, it helps to save network bandwidth.

### Configuration prerequisites

- Configuring parameters for the related interfaces
- Configuring link layer attributes for the related interfaces

- Enabling IPv6 packet forwarding
- Ensuring that the neighboring nodes are IPv6 reachable

### Configuring an IPv6 Static Route

Follow these steps to configure an IPv6 static route:

| To do… | Use the commands… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure an IPv6 static route | **ipv6 route-static** *ipv6-address prefix-length* [ *interface-type interface-number* ] *nexthop-address* [ **preference** *preference-value* ] | Required<br>The default preference of IPv6 static routes is 60. |

## Displaying and Maintaining IPv6 Static Routes

| To do… | Use the command… | Remarks |
|---|---|---|
| Display IPv6 static route information | **display ipv6 routing-table protocol static** [ **inactive** \| **verbose** ] | Available in any view |
| Remove all IPv6 static routes | **delete ipv6 static-routes all** | Available in system view |

**Note**

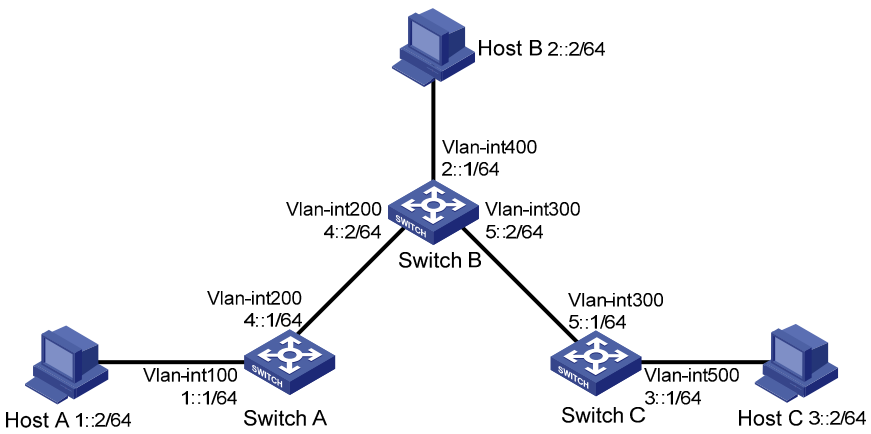
Using the **undo ipv6 route-static** command can delete a single IPv6 static route, while using the **delete ipv6 static-routes all** command deletes all IPv6 static routes including the default route.

## IPv6 Static Routing Configuration Example

### Network requirements

With IPv6 static routes configured, all hosts and switches can interact with each other.

**Figure 1-1** Network diagram for static routes



## Configuration procedure

1) Configure the IPv6 addresses of all VLAN interfaces (Omitted)
2) Configure IPv6 static routes.

# Configure the default IPv6 static route on SwitchA.

```
<SwitchA> system-view
[SwitchA] ipv6 route-static :: 0 4::2
```

# Configure two IPv6 static routes on SwitchB.

```
<SwitchB> system-view
[SwitchB] ipv6 route-static 1:: 64 4::1
[SwitchB] ipv6 route-static 3:: 64 5::1
```

# Configure the default IPv6 static route on SwitchC.

```
<SwitchC> system-view
[SwitchC] ipv6 route-static :: 0 5::2
```

3) Configure the IPv6 addresses of hosts and gateways.

Configure the IPv6 addresses of all the hosts based upon the network diagram, configure the default gateway of Host A as 1::1, that of Host B as 2::1, and that of Host C as 3::1.

4) Display configuration information

# Display the IPv6 routing table of SwitchA.

```
[SwitchA] display ipv6 routing-table
Routing Table :
         Destinations : 5        Routes : 5

 Destination  : :: /128                          Protocol     : Static
 NextHop      : FE80::510A:0:8D7:1               Preference   : 60
 Interface    : Vlan-interface200                Cost         : 0

 Destination  : ::1/128                          Protocol     : Direct
 NextHop      : ::1                              Preference   : 0
 Interface    : InLoop0                          Cost         : 0

 Destination  : 1:: /64                          Protocol     : Direct
 NextHop      : 1::1                             Preference   : 0
 Interface    : Vlan-interface100                Cost         : 0

 Destination  : 1::1/128                         Protocol     : Direct
 NextHop      : ::1                              Preference   : 0
 Interface    : InLoop0                          Cost         : 0

 Destination  : FE80::/10                        Protocol     : Direct
 NextHop      : ::                               Preference   : 0
 Interface    : NULL0                            Cost         : 0
```

# Verify the connectivity with the **ping** command.

```
[SwitchA] ping ipv6 3::1
  PING 3::1 : 56  data bytes, press CTRL_C to break
```

```
  Reply from 3::1
  bytes=56 Sequence=1 hop limit=254  time = 63 ms
  Reply from 3::1
  bytes=56 Sequence=2 hop limit=254  time = 62 ms
  Reply from 3::1
  bytes=56 Sequence=3 hop limit=254  time = 62 ms
  Reply from 3::1
  bytes=56 Sequence=4 hop limit=254  time = 63 ms
  Reply from 3::1
  bytes=56 Sequence=5 hop limit=254  time = 63 ms

--- 3::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/62/63 ms
```

# Table of Contents

# 1 RIPng Configuration

When configuring RIPng, go to these sections for information you are interested in:



**Note**

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

## Introduction to RIPng

RIP next generation (RIPng) is an extension of RIP-2 for IPv4. Most RIP concepts are applicable in RIPng.

RIPng for IPv6 has the following basic differences from RIP:

- UDP port number: RIPng uses UDP port 521 for sending and receiving routing information.
- Multicast address: RIPng uses FF02:9 as the link-local-router multicast address.
- Destination Prefix: 128-bit destination address prefix.
- Next hop: 128-bit IPv6 address.
- Source address: RIPng uses FE80::/10 as the link-local source address

### RIPng Working Mechanism

RIPng is a routing protocol based on the distance vector (D-V) algorithm. RIPng uses UDP packets to exchange routing information through port 521.

RIPng uses a hop count to measure the distance to a destination. The hop count is referred to as metric or cost. The hop count from a router to a directly connected network is 0. The hop count between two directly connected routers is 1. When the hop count is greater than or equal to 16, the destination network or host is unreachable.

By default, the routing update is sent every 30 seconds. If the router receives no routing updates from a neighbor within 180 seconds, the routes learned from the neighbor are considered as unreachable. Within another 240 seconds, if no routing update is received, the router will remove these routes from the routing table.

RIPng supports split horizon and poison reverse to prevent routing loops and route redistribution.

Each RIPng router maintains a routing database, including route entries of all reachable destinations. A route entry contains the following information:

- Destination address: IPv6 address of a host or a network.
- Next hop address: IPv6 address of a neighbor along the path to the destination.
- Egress interface: Outbound interface that forwards IPv6 packets.
- Metric: Cost from the local router to the destination.
- Route time: Time that elapsed since a route entry is last changed. Each time a route entry is modified, the routing time is set to 0.
- Route tag: Identifies the route, used in a routing policy to control routing information. For information about routing policy, refer to *Routing Policy Configuration* in the *IP Routing Volume*.

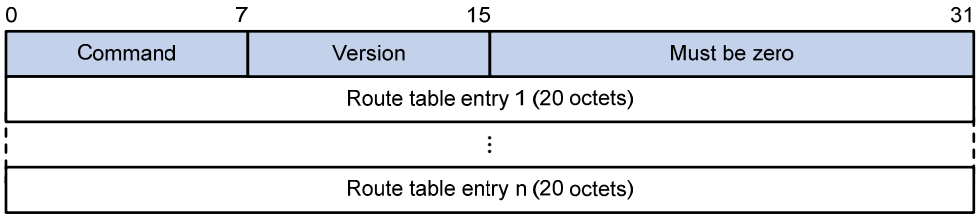
## RIPng Packet Format

### Basic format

A RIPng packet consists of a header and multiple route table entries (RTEs). The maximum number of RTEs in a packet depends on the IPv6 MTU of the sending interface.

Figure 1-1 shows the packet format of RIPng.

**Figure 1-1** RIPng basic packet format




- Command: Type of message. 0x01 indicates Request, 0x02 indicates Response.
- Version: Version of RIPng. It can only be 0x01 currently.
- RTE: Route table entry, 20 bytes for each entry.

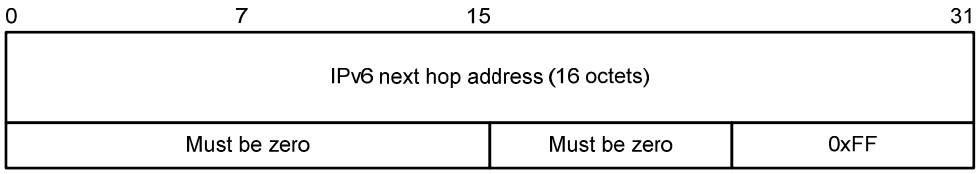
### RTE format

There are two types of RTEs in RIPng.

- Next hop RTE: Defines the IPv6 address of a next hop
- IPv6 prefix RTE: Describes the destination IPv6 address, route tag, prefix length and metric in the RIPng routing table.

Figure 1-2 shows the format of the next hop RTE:

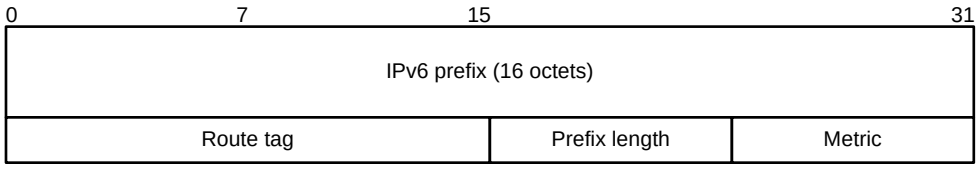
**Figure 1-2** Next hop RTE format




IPv6 next hop address is the IPv6 address of the next hop.

Figure 1-3 shows the format of the IPv6 prefix RTE.

**Figure 1-3** IPv6 prefix RTE format




- IPv6 prefix: Destination IPv6 address prefix.
- Route tag: Route tag.
- Prefix len: Length of the IPv6 address prefix.
- Metric: Cost of a route.

## RIPng Packet Processing Procedure

### Request packet

When a RIPng router first starts or needs to update some entries in its routing table, generally a multicast request packet is sent to ask for needed routes from neighbors.

The receiving RIPng router processes RTEs in the request. If there is only one RTE with the IPv6 prefix and prefix length both being 0, and with a metric value of 16, the RIPng router will respond with the entire routing table information in response messages. If there are multiple RTEs in the request message, the RIPng router will examine each RTE, update its metric, and send the requested routing information to the requesting router in the response packet.

### Response packet

The response packet containing the local routing table information is generated as:

- A response to a request
- An update periodically
- A trigged update caused by route change

After receiving a response, a router checks the validity of the response before adding the route to its routing table, such as whether the source IPv6 address is the link-local address and whether the port number is correct. The response packet that failed the check will be discarded.

## Protocols and Standards

- RFC 2080: RIPng for IPv6
- RFC 2081: RIPng Protocol Applicability Statement

# Configuring RIPng Basic Functions

This section presents the information to configure the basic RIPng features.

You need to enable RIPng first before configuring other tasks, but it is not necessary for RIPng related interface configurations, such as assigning an IPv6 address.

## Configuration Prerequisites

Before the configuration, accomplish the following tasks first:

- Enable IPv6 packet forwarding.

- Configure an IP address for each interface, and make sure all nodes are reachable to one another.

### Configuration Procedure

Follow these steps to configure the basic RIPng functions:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RIPng process and enter RIPng view | **ripng** [ *process-id* ] | Required<br>Not created by default |
| Return to system view | **quit** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable RIPng on the interface | **ripng** *process-id* **enable** | Required<br>Disabled by default |

**Note**

If RIPng is not enabled on an interface, the interface will not send or receive any RIPng route.

## Configuring RIPng Route Control

This section covers the following topics:

- Configuring RIPng Route Summarization
- Advertising a Default Route
- Configuring a RIPng Route Filtering Policy
- Configuring a Priority for RIPng
- Configuring RIPng Route Redistribution

Before the configuration, accomplish the following tasks first:

- Configure an IPv6 address on each interface, and make sure all nodes are reachable to one another.
- Configure RIPng basic functions
- Define an IPv6 ACL before using it for route filtering. Refer to *ACL Configuration* in the *Security Volume* for related information.
- Define an IPv6 address prefix list before using it for route filtering. Refer to *Routing Policy Configuration* in the *IP Routing Volume* for related information.

### Configuring an Additional Routing Metric

An additional routing metric can be added to the metric of an inbound or outbound RIP route, namely, the inbound and outbound additional metric.

The outbound additional metric is added to the metric of a sent route. The route's metric in the routing table is not changed.

The inbound additional metric is added to the metric of a received route before the route is added into the routing table, so the route's metric is changed.

Follow these steps to configure an inbound/outbound additional routing metric:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Specify an inbound routing additional metric | **ripng metricin** *value* | Optional<br>0 by default |
| Specify an outbound routing additional metric | **ripng metricout** *value* | Optional<br>1 by default |

## Configuring RIPng Route Summarization

Follow these steps to configure RIPng route summarization:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Advertise a summary IPv6 prefix | **ripng summary-address** *ipv6-address prefix-length* | Required |

## Advertising a Default Route

Follow these steps to advertise a default route:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Advertise a default route | **ripng default-route** { **only** \| **originate** } [ **cost** *cost* ] | Required<br>Not advertised by default |

**Note**

With this feature enabled, a default route is advertised through the specified interface regardless of whether the default route is available in the local IPv6 routing table.

## Configuring a RIPng Route Filtering Policy

You can reference a configured IPv6 ACL or prefix list to filter received/advertised routing information as needed. For filtering outbound routes, you can also specify a routing protocol from which to filter routing information redistributed.

Follow these steps to configure a RIPng route filtering policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIPng view | **ripng** [ *process-id* ] | — |
| Configure a filter policy to filter incoming routes | **filter-policy** { *acl6-number* \| **ipv6-prefix** *ipv6-prefix-name* } **import** | Required<br>By default, RIPng does not filter incoming routing information. |
| Configure a filter policy to filter outgoing routes | **filter-policy** { *acl6-number* \| **ipv6-prefix** *ipv6-prefix-name* } **export** [ *protocol* [ *process-id* ] ] | Required<br>By default, RIPng does not filter outgoing routing information. |

## Configuring a Priority for RIPng

Any routing protocol has its own protocol priority used for optimal route selection. You can set a priority for RIPng manually. The smaller the value is, the higher the priority is.

Follow these steps to configure a RIPng priority:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIPng view | **ripng** [ *process-id* ] | — |
| Configure a RIPng priority | **preference** [ **route-policy** *route-policy-name* ] *preference* | Optional<br>By default, the RIPng priority is 100. |

## Configuring RIPng Route Redistribution

Follow these steps to configure RIPng route redistribution:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIPng view | **ripng** [ *process-id* ] | — |
| Configure a default routing metric for redistributed routes | **default cost** *cost* | Optional<br>The default metric of redistributed routes is 0. |
| Redistribute routes from another routing protocol | **import-route** *protocol* [ *process-id* ] [ **allow-ibgp** ] [ **cost** *cost* \| **route-policy** *route-policy-name* ] * | Required<br>No route redistribution is configured by default. |

# Tuning and Optimizing the RIPng Network

This section describes how to tune and optimize the performance of the RIPng network as well as applications under special network environments. Before tuning and optimizing the RIPng network, complete the following tasks:

- Configure a network layer address for each interface
- Configure the basic RIPng functions

This section covers the following topics:



## Configuring RIPng Timers

You can adjust RIPng timers to optimize the performance of the RIPng network.

Follow these steps to configure RIPng timers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIPng view | **ripng** [ *process-id* ] | — |
| Configure RIPng timers | **timers** { **garbage-collect** *garbage-collect-value* \| **suppress** *suppress-value* \| **timeout** *timeout-value* \| **update** *update-value* } * | Optional.<br>The RIPng timers have the following defaults:<br>• 30 seconds for the update timer<br>• 180 seconds for the timeout timer<br>• 120 seconds for the suppress timer<br>• 120 seconds for the garbage-collect timer |

**Note**

When adjusting RIPng timers, you should consider the network performance and perform unified configurations on routers running RIPng to avoid unnecessary network traffic increase or route oscillation.

## Configuring Split Horizon and Poison Reverse

**Note**

If both split horizon and poison reverse are configured, only the poison reverse function takes effect.

### Configure split horizon

The split horizon function disables a route learned from an interface from being advertised through the

same interface to prevent routing loops between neighbors.

Follow these steps to configure split horizon:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the split horizon function | **ripng split-horizon** | Optional<br>Enabled by default |

**Note**

Generally, you are recommended to enable split horizon to prevent routing loops.

### Configuring the poison reverse function

The poison reverse function enables a route learned from an interface to be advertised through the interface. However, the metric of the route is set to 16. That is to say, the route is unreachable.

Follow these steps to configure poison reverse:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the poison reverse function | **ripng poison-reverse** | Required<br>Disabled by default |

## Configuring Zero Field Check on RIPng Packets

Some fields in the RIPng packet must be zero. These fields are called zero fields. With zero field check on RIPng packets enabled, if such a field contains a non-zero value, the entire RIPng packet will be discarded. If you are sure that all packets are trusty, you can disable the zero field check to reduce the CPU processing time.

Follow these steps to configure RIPng zero field check:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter RIPng view | **ripng** [ *process-id* ] | — |
| Enable the zero field check | **checkzero** | Optional<br>Enabled by default |

# Displaying and Maintaining RIPng

| To do… | Use the command… | Remarks |
|---|---|---|
| Display configuration information of a RIPng process | **display ripng** [ *process-id* ] | Available in any view |
| Display routes in the RIPng database | **display ripng** *process-id* **database** | Available in any view |
| Display the routing information of a specified RIPng process | **display ripng** *process-id* **route** | Available in any view |
| Display RIPng interface information | **display ripng** *process-id* **interface** [ *interface-type interface-number* ] | Available in any view |

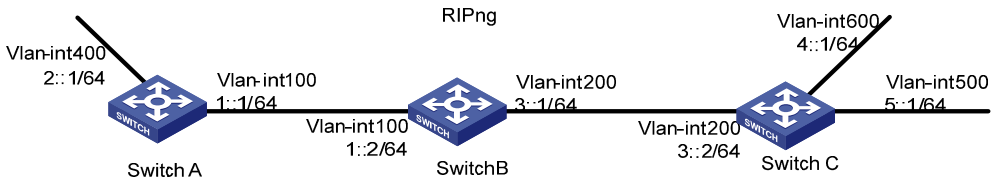
# RIPng Configuration Example

## Configure RIPng Basic Functions

### Network requirements

As shown in Figure 1-4, all switches run RIPng. Configure Switch B to filter the route (3::/64) learnt from Switch C, which means the route will not be added to the routing table of Switch B, and Switch B will not forward it to Switch A.

**Figure 1-4** Network diagram for RIPng configuration




### Configuration procedure

1) Configure the IPv6 address for each interface (omitted)
2) Configure basic RIPng functions

# Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ripng 1 enable
[SwitchA-Vlan-interface400] quit
```

# Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
```

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

# Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 500
[SwitchC-Vlan-interface500] ripng 1 enable
[SwitchC-Vlan-interface500] quit
[SwitchC] interface vlan-interface 600
[SwitchC-Vlan-interface600] ripng 1 enable
[SwitchC-Vlan-interface600] quit
```

# Display the routing table of Switch B.

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::20F:E2FF:FE23:82F5  on Vlan-interface100
 Dest 1::/64,
     via FE80::20F:E2FF:FE23:82F5, cost  1, tag 0, A, 6 Sec
 Dest 2::/64,
     via FE80::20F:E2FF:FE23:82F5, cost  1, tag 0, A, 6 Sec

 Peer FE80::20F:E2FF:FE00:100  on Vlan-interface200
 Dest 3::/64,
     via FE80::20F:E2FF:FE00:100, cost  1, tag 0, A, 11 Sec
 Dest 4::/64,
     via FE80::20F:E2FF:FE00:100, cost  1, tag 0, A, 11 Sec
 Dest 5::/64,
     via FE80::20F:E2FF:FE00:100, cost  1, tag 0, A, 11 Sec
```

# Display the routing table of Switch A.

```
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::200:2FF:FE64:8904  on Vlan-interface100
 Dest 1::/64,
     via FE80::200:2FF:FE64:8904, cost  1, tag 0, A, 31 Sec
 Dest 4::/64,
```

```
     via FE80::200:2FF:FE64:8904, cost  2, tag 0, A, 31 Sec
 Dest 5::/64,
     via FE80::200:2FF:FE64:8904, cost  2, tag 0, A, 31 Sec
 Dest 3::/64,
     via FE80::200:2FF:FE64:8904, cost  1, tag 0, A, 31 Sec
```

3) Configure Switch B to filter incoming and outgoing routes.

```
[SwitchB] acl ipv6 number 2000
[SwitchB-acl6-basic-2000] rule deny source 3::/64
[SwitchB-acl6-basic-2000] rule permit
[SwitchB-acl6-basic-2000] quit
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy 2000 import
[SwitchB-ripng-1] filter-policy 2000 export
```

# Display routing tables of Switch B and Switch A.

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::20F:E2FF:FE23:82F5  on Vlan-interface100
 Dest 1::/64,
     via FE80::20F:E2FF:FE23:82F5, cost  1, tag 0, A, 2 Sec
 Dest 2::/64,
     via FE80::20F:E2FF:FE23:82F5, cost  1, tag 0, A, 2 Sec

 Peer FE80::20F:E2FF:FE00:100  on Vlan-interface200
 Dest 4::/64,
     via FE80::20F:E2FF:FE00:100, cost  1, tag 0, A, 5 Sec
 Dest 5::/64,
     via FE80::20F:E2FF:FE00:100, cost  1, tag 0, A, 5 Sec
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::20F:E2FF:FE00:1235  on Vlan-interface100
 Dest 1::/64,
     via FE80::20F:E2FF:FE00:1235, cost  1, tag 0, A, 2 Sec
 Dest 4::/64,
     via FE80::20F:E2FF:FE00:1235, cost  2, tag 0, A, 2 Sec
 Dest 5::/64,
     via FE80::20F:E2FF:FE00:1235, cost  2, tag 0, A, 2 Sec
```

# Table of Contents

# 1 Route Policy Configuration

A route policy is used on a router for route filtering and attributes modification when routes are received, advertised, or redistributed.

When configuring route policy, go to these sections for information you are interested in:



**Note**

Route policy in this chapter involves both IPv4 route policy and IPv6 route policy.

## Introduction to Route Policy

### Route Policy

A route policy is used on a router for route filtering and attributes modification when routes are received, advertised, or redistributed.

To configure a route policy, you need to define some filters based on the attributes of routing information, such as destination address, advertising router's address and so on. The filters can be set beforehand and then applied to the route policy.

### Filters

There are six types of filters: ACL, IP prefix list, and route policy.

#### ACL

ACL involves IPv4 ACL and IPv6 ACL. An ACL is configured to match the destinations or next hops of routing information.

For ACL configuration, refer to *ACL configuration* in the *Security Volume*.

#### IP prefix list

IP prefix list involves IPv4 and IPv6 prefix list.

An IP prefix list is configured to match the destination address of routing information. Moreover, you can use the **gateway** option to allow only routing information from certain routers to be received. For **gateway** option information, refer to *RIP Commands* in the *IP Routing Volume.*

An IP prefix list, identified by name, can comprise multiple items. Each item, identified by an index number, can specify a prefix range to match. An item with a smaller index number is matched first. If one item is matched, the IP prefix list is passed, and the packet will not go to the next item.

#### Route policy

A route policy is used to match routing information and modify the attributes of permitted routes. It can reference the above mentioned filters to define its own match criteria.

A route policy can comprise multiple nodes, which are in logic OR relationship. Each route policy node is a match unit, and a node with a smaller number is matched first. Once a node is matched, the route policy is passed and the packet will not go to the next node.

A route policy node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the match criteria. The matching objects are some attributes of routing information. The **if-match** clauses of a route policy node is in logical AND relationship. That is, a packet must match all the **if-match** clauses of the node to pass it. The **apply** clauses of the node specify the actions to be taken on the permitted packets, such as route attribute modification.

### Route Policy Application

A route policy is applied on a router to filter routes when they are received, advertised or redistributed and to modify some attributes of permitted routes.

## Route Policy Configuration Task List

Complete the following tasks to configure a route policy:

| Task | |
|---|---|
| Defining Filters | Defining an IP-prefix List |
| Configuring a Route Policy | Creating a Route Policy |
| | Defining if-match Clauses |
| | Defining apply Clauses |

## Defining Filters

### Prerequisites

Before configuring this task, you need to decide on:

- IP-prefix list name
- Matching address range

## Defining an IP-prefix List

### Define an IPv4 prefix list

Identified by name, an IPv4 prefix list can comprise multiple items. Each item specifies a prefix range to match and is identified by an index number.

An item with a smaller index number is matched first. If one item is matched, the IP prefix list is passed, and the routing information will not go to the next item.

Follow these steps to define an IPv4 prefix list:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Define an IPv4 prefix list | **ip ip-prefix** *ip-prefix-name* [ **index** *index-number* ] { **permit** \| **deny** } *ip-address mask-length* [ **greater-equal** *min-mask-length* ] [ **less-equal** *max-mask-length* ] | Required<br>Not defined by default. |

**Note**

If all the items are set to the **deny** mode, no routes can pass the IPv4 prefix list. Therefore, you need to define the **permit** 0.0.0.0 0 **less-equal** 32 item following multiple **deny** items to allow other IPv4 routing information to pass.

For example, the following configuration filters routes 10.1.0.0/16, 10.2.0.0/16 and 10.3.0.0/16, but allows other routes to pass.

```
<Sysname> system-view
[Sysname] ip ip-prefix abc index 10 deny 10.1.0.0 16
[Sysname] ip ip-prefix abc index 20 deny 10.2.0.0 16
[Sysname] ip ip-prefix abc index 30 deny 10.3.0.0 16
[Sysname] ip ip-prefix abc index 40 permit 0.0.0.0 0 less-equal 32
```

### Define an IPv6 prefix list

Identified by name, each IPv6 prefix list can comprise multiple items. Each item specifies a prefix range to match and is identified by an index number.

An item with a smaller index number is matched first. If one item is matched, the IPv6 prefix list is passed, and the routing information will not go to the next item.

Follow these steps to define an IPv6 prefix list:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Define an IPv6 prefix list | **ip ipv6-prefix** *ipv6-prefix-name* [ **index** *index-number* ] { **deny** \| **permit** } *ipv6-address prefix-length* [ **greater-equal** *min-prefix-length* ] [ **less-equal** *max-prefix-length* ] | Required<br>Not defined by default. |

**Note**

If all items are set to the **deny** mode, no routes can pass the IPv6 prefix list. Therefore, you need to define the **permit** :: 0 **less-equal** 128 item following multiple **deny** items to allow other IPv6 routing information to pass.

For example, the following configuration filters routes 2000:1::/48, 2000:2::/48 and 2000:3::/48, but allows other routes to pass.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc index 10 deny 2000:1:: 48
[Sysname] ip ipv6-prefix abc index 20 deny 2000:2:: 48
[Sysname] ip ipv6-prefix abc index 30 deny 2000:3:: 16
[Sysname] ip ipv6-prefix abc index 40 permit :: 0 less-equal 128
```

# Configuring a Route Policy

A route policy is used to filter routing information, and modify attributes of matching routing information. The match criteria of a route policy can be configured by referencing filters above mentioned.

A route policy can comprise multiple nodes, and each route policy node contains:

- **if-match** clauses: Define the match criteria that routing information must satisfy. The matching objects are some attributes of routing information.
- **apply** clauses: Specify the actions to be taken on routing information that has satisfied the match criteria, such as route attribute modification.

## Prerequisites

Before configuring this task, you need to configure:

- Filters
- Routing protocols

You also need to decide on:

- Name of the route policy, and node numbers
- Match criteria
- Attributes to be modified

## Creating a Route Policy

Follow these steps to create a route policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a route policy, specify a node for it and enter route policy node view | **route-policy** *route-policy-name* { **permit** \| **deny** } **node** *node-number* | Required |

**Note**

- If a route policy node has the **permit** keyword specified, routing information matching all the **if-match** clauses of the node will be handled using the **apply** clauses of this node, without needing to match against the next node. If routing information does not match the node, it will go to the next node for a match.
- If a route policy node has the **deny** keyword specified, the **apply** clauses of the node will not be executed. When routing information matches all the **if-match** clauses of the node, it cannot pass the node, or go to the next node. If route information cannot match all the **if-match** clauses of the node, it will go to the next node for a match.
- When a route policy has more than one node, at least one node should be configured with the **permit** keyword. If the route policy is used to filter routing information, routing information that does not meet any node cannot pass the route policy. If all nodes of the route policy are set with the **deny** keyword, no routing information can pass it.

## Defining if-match Clauses

Follow these steps to define if-match clauses for a route-policy node:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter route policy node view | | **route-policy** *route-policy-name* { **permit** \| **deny** } **node** *node-number* | Required |
| Define match criteria for IPv4 routes | Match IPv4 routing information specified in the ACL | **if-match acl** *acl-number* | Optional<br>Not configured by default. |
| | Match IPv4 routing information specified in the IP prefix list | **if-match ip-prefix** *ip-prefix-name* | |
| | Match IPv4 routing information whose next hop or source is specified in the ACL or IP prefix list | **if-match ip** { **next-hop** \| **route-source** } { **acl** *acl-number* \| **ip-prefix** *ip-prefix-name* } | Optional<br>Not configured by default. |
| Match IPv6 routing information whose next hop or source is specified in the ACL or IP prefix list | | **if-match ipv6** { **address** \| **next-hop** \| **route-source** } { **acl** *acl-number* \| **prefix-list** *ipv6-prefix-name* } | Optional<br>Not configured by default. |
| Match routes having the specified cost | | **if-match cost** *value* | Optional<br>Not configured by default. |
| Match routing information having specified outbound interface(s) | | **if-match interface** { *interface-type interface-number* }&<1-16> | Optional<br>Not configured by default. |
| Match RIP routing information having the specified tag value | | **if-match tag** *value* | Optional<br>Not configured by default. |

**Note**

- The **if-match** clauses of a route policy node are in logic AND relationship, namely, routing information has to satisfy all its **if-match** clauses before being executed with its **apply** clauses.
- You can specify no or multiple **if-match** clauses for a route policy node. If no **if-match** clause is specified, and the route policy node is in **permit** mode, all routing information can pass the node. If it is in **deny** mode, no routing information can pass it.
- The **if-match** commands for matching IPv4 destination, next hop and source address are different from those for matching IPv6 ones.

## Defining apply Clauses

Follow these steps to define **apply** clauses for a route policy:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter route policy node view | | **route-policy** *route-policy-name* { **permit** \| **deny** } **node** *node-number* | Required<br>Not created by default. |
| Set the next hop | for IPv4 routes | **apply ip-address next-hop** *ip-address* | Optional<br>Not set by default.<br>The setting does not apply to redistributed routing information. |
| | for IPv6 routes | **apply ipv6 next-hop** *ipv6-address* | Optional<br>Not set by default.<br>The setting does not apply to redistributed routing information. |
| Set the preference for the routing protocol | | **apply preference** *preference* | Optional<br>Not set by default. |
| Set a tag value for RIP routing information | | **apply tag** *value* | Optional<br>Not set by default. |

**Note**

- The difference between IPv4 and IPv6 **apply** clauses is the command for setting the next hop for routing information.
- The **apply ip-address next-hop** and **apply ipv6 next-hop** commands do not apply to redistributed IPv4 and IPv6 routes respectively.

# Displaying and Maintaining the Route Policy

| To do… | Use the command… | Remarks |
|---|---|---|
| Display IPv4 prefix list statistics | **display ip ip-prefix** [ *ip-prefix-name* ] | Available in any view |
| Display IPv6 prefix list statistics | **display ip ipv6-prefix** [ *ipv6-prefix-name* ] | |
| Display route policy information | **display route-policy** [ *route-policy-name* ] | |
| Clear IPv4 prefix list statistics | **reset ip ip-prefix** [ *ip-prefix-name* ] | Available in user view |
| Clear IPv6 prefix list statistics | **reset ip ipv6-prefix** [ *ipv6-prefix-name* ] | |

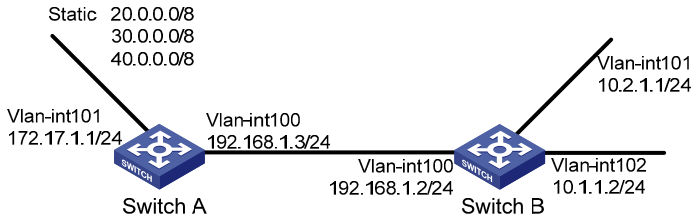
# Route Policy Configuration Example

## Applying a Route Policy to IPv4 Route Redistribution

### Network Requirements

As shown in the following figure, Switch A and Switch B communicate with each other at the network layer through RIPv2. Switch A has static routes to networks 20.0.0.0/8, 30.0.0.0/8, and 40.0.0.0/8. Switch B needs to access these networks through Switch A, while Switch A allows Switch B to access networks 20.0.0.0/8 and 40.0.0.0/8, but not 30.0.0.0/8.

**Figure 1-1** Network diagram for route policy application to route redistribution




### Configuration procedure

1) Configure Switch A.

# Configure IP addresses of the interfaces (omitted).

# Configure RIP basic functions.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] quit
```

# Configure three static routes.

```
[SwitchA] ip route-static 20.0.0.0 255.0.0.0 172.17.1.2
[SwitchA] ip route-static 30.0.0.0 255.0.0.0 172.17.1.2
[SwitchA] ip route-static 40.0.0.0 255.0.0.0 172.17.1.2
```

# Configure an ACL.

```
[SwitchA] acl number 2000
```

```
[SwitchA-acl-basic-2000] rule deny source 30.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule permit source any
[SwitchA-acl-basic-2000] quit
```

# Redistribute static routes.

```
[SwitchA] rip
[SwitchA-rip-1] import-route static
```

# Apply ACL 2000 to filter the routing information to be advertised to Switch B.

```
[SwitchA-rip-1] filter-policy 2000 export vlan-interface 100
[SwitchA-rip-1] quit
```

2) Configure Switch B.

# Configure IP addresses of the interfaces (omitted).

# Configure RIP basic functions.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 10.0.0.0
[SwitchB-rip-1] quit
```

3) Display the RIP routing table of Switch B and verify the configuration.

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P  -  Permanent,  A  -  Aging,  S  -  Suppressed,  G  -  Garbage-collect
------------------------------------------------------------------------
 Peer 192.168.1.3  on Vlan-interface100
      Destination/Mask        Nexthop     Cost    Tag    Flags   Sec
         20.0.0.0/8       192.168.1.3         1       0    RA      14
         40.0.0.0/8       192.168.1.3         1       0    RA      14
```

The display shows that Switch B has only the routing information permitted by ACL 2000. Therefore, the configurations above can meet the configuration requirements.

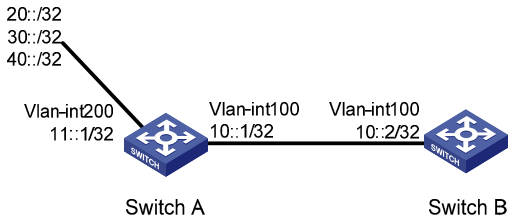
## Applying a Route Policy to IPv6 Route Redistribution

### Network requirements

As shown in the following figure:

- Enable RIPng on Switch A and Switch B.
- On Switch A, configure three static routes, and apply a route policy to static route redistribution to permit routes 20::0/32 and 40::0/32, and deny route 30::0/32.
- Display RIPng routing table information on Switch B to verify the configuration.

**Figure 1-2** Network diagram for route policy application to route redistribution




## Configuration procedure

1) Configure Switch A.

# Configure IPv6 addresses for VLAN-interface 100 and VLAN-interface 200.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 address 10::1 32
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ipv6 address 11::1 32
[SwitchA-Vlan-interface200] quit
```

# Enable RIPng on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

# Configure three static routes.

```
[SwitchA] ipv6 route-static 20:: 32 11::2
[SwitchA] ipv6 route-static 30:: 32 11::2
[SwitchA] ipv6 route-static 40:: 32 11::2
```

# Configure a route policy.

```
[SwitchA] ip ipv6-prefix a index 10 permit 30:: 32
[SwitchA] route-policy static2ripng deny node 0
[SwitchA-route-policy] if-match ipv6 address prefix-list a
[SwitchA-route-policy] quit
[SwitchA] route-policy static2ripng permit node 10
[SwitchA-route-policy] quit
```

# Enable RIPng and apply the route policy to static route redistribution.

```
[SwitchA] ripng
[SwitchA-ripng-1] import-route static route-policy static2ripng
```

2) Configure Switch B.

# Configure the IPv6 address for VLAN-interface 100.

```
[SwitchB] ipv6
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 10::2 32
```

# Enable RIPng on VLAN-interface 100.

```
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

# Enable RIPng.

```
[SwitchB] ripng
```

# Display RIPng routing table information.

```
[SwitchB-ripng-1] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::7D58:0:CA03:1  on Vlan-interface 100
 Dest 10::/32,
     via FE80::7D58:0:CA03:1, cost  1, tag 0, A, 18 Sec
 Dest 20::/32,
     via FE80::7D58:0:CA03:1, cost  1, tag 0, A, 8 Sec
 Dest 40::/32,
     via FE80::7D58:0:CA03:1, cost  1, tag 0, A, 3 Sec
```

# Troubleshooting Route Policy Configuration

## IPv4 Routing Information Filtering Failure

### Symptom

Filtering routing information failed, while the routing protocol runs normally.

### Analysis

At least one item of the IP prefix list should be configured as permit mode, and at least one node in the Route policy should be configured as permit mode.

### Solution

1) Use the **display ip ip-prefix** command to display IP prefix list information.
2) Use the **display route-policy** command to display route policy information.

## IPv6 Routing Information Filtering Failure

### Symptom

Filtering routing information failed, while the routing protocol runs normally.

### Analysis

At least one item of the IPv6 prefix list should be configured as permit mode, and at least one node of the Route policy should be configured as permit mode.

### Solution

1) Use the **display ip ipv6-prefix** command to display IP prefix list information.
2) Use the **display route-policy** command to display route policy information.

# IP Multicast Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The IP Multicast Volume is organized as follows:

| Features | Description |
|---|---|
| Multicast Overview | This document describes the main concepts in multicast:<br>• Introduction to Multicast<br>• Multicast Models<br>• Multicast Architecture<br>• Multicast Packets Forwarding Mechanism |
| IGMP Snooping | Running at the data link layer, IGMP Snooping is a multicast control mechanism on the Layer 2 Ethernet switch and it is used for multicast group management and control. This document describes:<br>• Configuring Basic Functions of IGMP Snooping<br>• Configuring IGMP Snooping Port Functions<br>• Configuring IGMP Snooping Querier<br>• Configuring IGMP Snooping Policy |
| Multicast VLAN | Multicast VLAN configuration |
| MLD Snooping | Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. This document describes:<br>• Configuring Basic Functions of MLD Snooping<br>• Configuring MLD Snooping Port Functions<br>• Configuring MLD Snooping Querier<br>• Configuring MLD Snooping Policy |
| IPv6 Multicast VLAN | IPv6 Multicast VLAN configuration |

# Table of Contents

# 1 Multicast Overview

**Note**

This manual chiefly focuses on the IP multicast technology and device operations. Unless otherwise stated, the term “multicast” in this document refers to IP multicast.

## Introduction to Multicast

As a technique coexisting with unicast and broadcast, the multicast technique effectively addresses the issue of point-to-multipoint data transmission. By allowing high-efficiency point-to-multipoint data transmission over a network, multicast greatly saves network bandwidth and reduces network load.

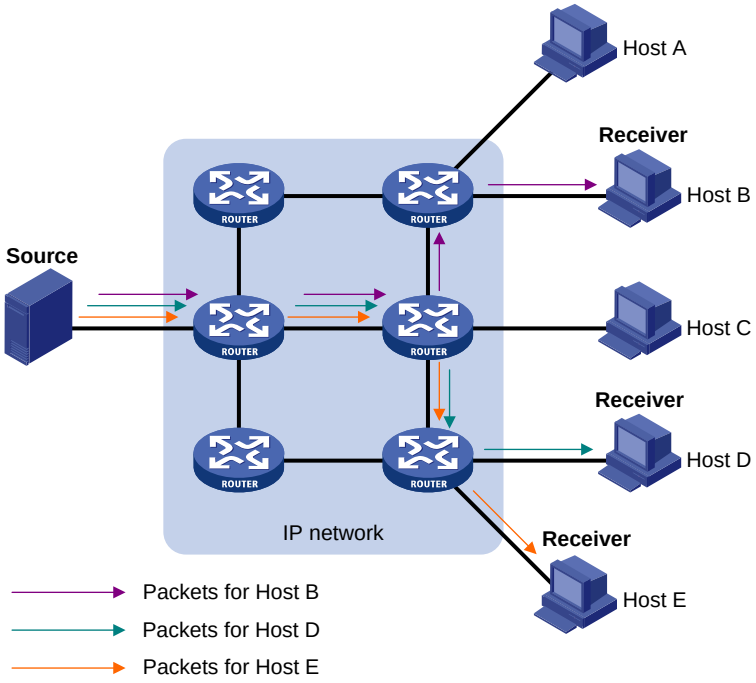
With the multicast technology, a network operator can easily provide new value-added services, such as live Webcasting, Web TV, distance learning, telemedicine, Web radio, real-time videoconferencing, and other bandwidth- and time-critical information services.

### Comparison of Information Transmission Techniques

#### Unicast

In unicast, the information source (Source in the figure) needs to send a separate copy of information to each host (Receiver in the figure) that wants the information, as shown in Figure 1-1.

**Figure 1-1** Unicast transmission




Assume that Host B, Host D and Host E need the information. A separate transmission channel needs to be established from the information source to each of these hosts.

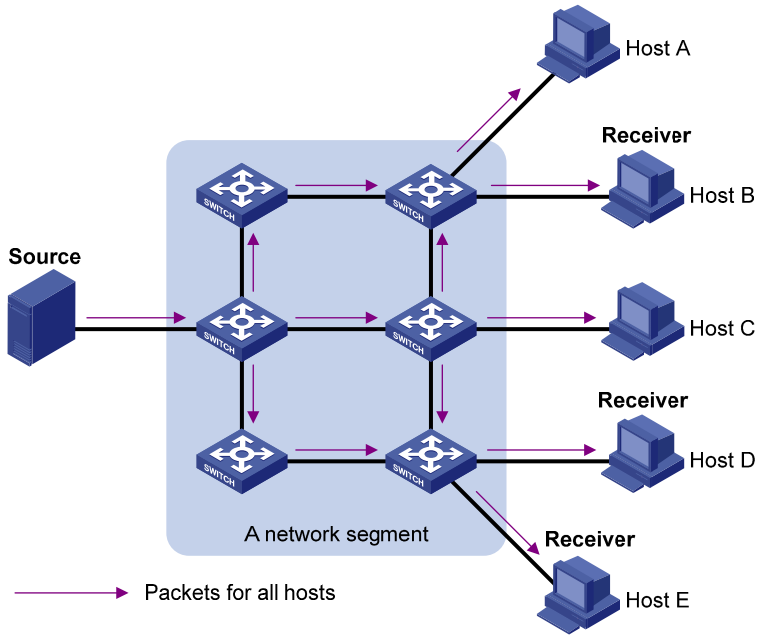
In unicast transmission, the traffic transmitted over the network is proportional to the number of hosts that need the information. If a large number of users need the information, the information source needs to send a copy of the same information to each of these users. This means a tremendous pressure on the information source and the network bandwidth.

As we can see from the information transmission process, unicast is not suitable for batch transmission of information.

## Broadcast

In broadcast, the information source sends information to all hosts on the subnet, even if some hosts do not need the information, as shown in Figure 1-2.

**Figure 1-2** Broadcast transmission




Assume that only Host B, Host D, and Host E need the information. If the information is broadcast to the subnet, Host A and Host C also receive it. In addition to information security issues, this also causes traffic flooding on the same subnet.

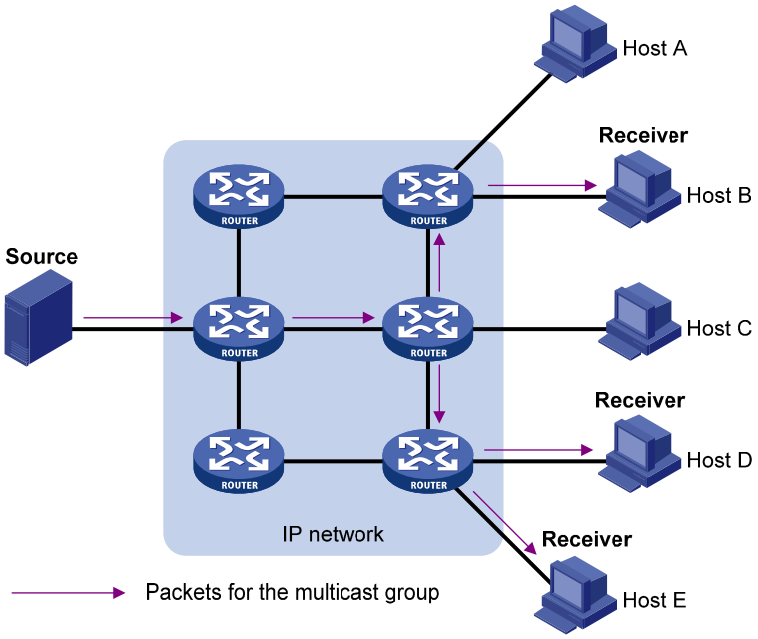
Therefore, broadcast is disadvantageous in transmitting data to specific hosts; moreover, broadcast transmission is a significant waste of network resources.

## Multicast

As discussed above, unicast and broadcast techniques are unable to provide point-to-multipoint data transmissions with the minimum network consumption.

Multicast can well solve this problem. When some hosts on the network need multicast information, the information sender, or multicast source, sends only one copy of the information. Multicast distribution trees are built through multicast routing protocols, and the packets are replicated only on nodes where the trees branch. Figure 1-3 shows the delivery of a data stream to receiver hosts through multicast.

**Figure 1-3** Multicast transmission




The multicast source (Source in the figure) sends only one copy of the information to a multicast group. Host B, Host D and Host E, which are receivers of the information, need to join the multicast group. The routers on the network duplicate and forward the information based on the distribution of the group members. Finally, the information is correctly delivered to Host B, Host D, and Host E.

To sum up, the advantages of multicast are summarized as follows:

- Over unicast: As multicast traffic flows to the node the farthest possible from the source before it is replicated and distributed, an increase of the number of hosts will not increase the load of the source and will not remarkably add to network resource usage.
- Over broadcast: As multicast data is sent only to the receivers that need it, multicast uses the network bandwidth reasonably and enhances network security. In addition, data broadcast is confined to the same subnet, while multicast is not.

## Features of Multicast

Multicast has the following features:

- A multicast group is a multicast receiver set identified by an IP multicast address. Hosts join a multicast group to become members of the multicast group, before they can receive the multicast data addressed to that multicast group. Typically, a multicast source does not need to join a multicast group.
- An information sender is referred to as a multicast source (Source in Figure 1-3). A multicast source can send data to multiple multicast groups at the same time, and multiple multicast sources can send data to the same multicast group at the same time.
- All hosts that have joined a multicast group become members of the multicast group (Receiver in Figure 1-3). The group memberships are dynamic. Hosts can join or leave multicast groups at any time. Multicast groups are not subject to geographic restrictions.
- Routers or Layer 3 switches that support Layer 3 multicast are called multicast routers or Layer 3 multicast devices. In addition to providing the multicast routing function, a multicast router can also manage multicast group memberships on stub subnets with attached group members. A multicast router itself can be a multicast group member.

For a better understanding of the multicast concept, you can assimilate multicast transmission to the transmission of TV programs, as shown in Table 1-1.

**Table 1-1** An analogy between TV transmission and multicast transmission

| TV transmission | Multicast transmission |
|---|---|
| A TV station transmits a TV program through a channel. | A multicast source sends multicast data to a multicast group. |
| A user tunes the TV set to the channel. | A receiver joins the multicast group. |
| The user starts to watch the TV program transmitted by the TV station via the channel. | The receiver starts to receive the multicast data that the source is sending to the multicast group. |
| The user turns off the TV set or tunes to another channel. | The receiver leaves the multicast group or joins another group. |

## Common Notations in Multicast

Two notations are commonly used in multicast:

- (*, G): Indicates a rendezvous point tree (RPT), or a multicast packet that any multicast source sends to multicast group G. Here “*” represents any multicast source, while “G” represents a specific multicast group.
- (S, G): Indicates a shortest path tree (SPT), or a multicast packet that multicast source S sends to multicast group G. Here “S” represents a specific multicast source, while “G” represents a specific multicast group.

## Advantages and Applications of Multicast

### Advantages of multicast

Advantages of the multicast technique include:

- Enhanced efficiency: reduces the CPU load of information source servers and network devices.
- Optimal performance: reduces redundant traffic.
- Distributive application: enables point-to-multipoint applications at the price of minimum network resources.

### Applications of multicast

Applications of the multicast technique include:

- Multimedia and streaming applications, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as distance learning and telemedicine.
- Data warehouse and financial applications (stock quotes).
- Any other point-to-multipoint data distribution application.

# Multicast Models

Based on how the receivers treat the multicast sources, there are three multicast models: any-source multicast (ASM), source-filtered multicast (SFM), and source-specific multicast (SSM).

### ASM model

In the ASM model, any sender can send information to a multicast group as a multicast source, and numbers of receivers can join a multicast group identified by a group address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the position of multicast sources in advance. However, they can join or leave the multicast group at any time.

### SFM model

The SFM model is derived from the ASM. From the view of a sender, the two models have the same multicast membership architecture.

The SFM model functionally extends the ASM model: In the SFM model, the upper layer software checks the source address of received multicast packets and permits or denies multicast traffic from specific sources. Therefore, receivers can receive the multicast data from only part of the multicast sources. From the view of a receiver, multicast sources are not all valid: they are filtered.

### SSM model

In the practical life, users may be interested in the multicast data from only certain multicast sources. The SSM model provides a transmission service that allows users to specify the multicast sources they are interested in at the client side.

The radical difference between the SSM model and the ASM model is that in the SSM model, receivers already know the locations of the multicast sources by some other means. In addition, the SSM model uses a multicast address range that is different from that of the ASM/SFM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

## Multicast Architecture

IP multicast addresses the following questions:

- Where should the multicast source transmit information to? (multicast addressing)
- What receivers exist on the network? (host registration)
- Where is the multicast source the receivers need to receive multicast data from? (multicast source discovery)
- How should information be transmitted to the receivers? (multicast routing)

IP multicast falls in the scope of end-to-end service. The multicast architecture involves the following four parts:

1) Addressing mechanism: Information is sent from a multicast source to a group of receivers through a multicast address.
2) Host registration: Receiver hosts are allowed to join and leave multicast groups dynamically. This mechanism is the basis for group membership management.
3) Multicast routing: A multicast distribution tree (namely a forwarding path tree for multicast data on the network) is constructed for delivering multicast data from a multicast source to receivers.
4) Multicast applications: A software system that supports multicast applications, such as video conferencing, must be installed on multicast sources and receiver hosts, and the TCP/IP stack must support reception and transmission of multicast data.

## Multicast Addresses

To allow communication between multicast sources and multicast group members, network-layer multicast addresses, namely, multicast IP addresses must be provided. In addition, a technique must be available to map multicast IP addresses to link-layer multicast MAC addresses.

### IP multicast addresses

1) IPv4 multicast addresses

Internet Assigned Numbers Authority (IANA) assigned the Class D address space (224.0.0.0 to 239.255.255.255) for IPv4 multicast. The specific address blocks and usages are shown in Table 1-2.

**Table 1-2** Class D IP address blocks and description

| Address block | Description |
|---|---|
| 224.0.0.0 to 224.0.0.255 | Reserved permanent group addresses. The IP address 224.0.0.0 is reserved, and other IP addresses can be used by routing protocols and for topology searching, protocol maintenance, and so on. Common permanent group addresses are listed in Table 1-3. A packet destined for an address in this block will not be forwarded beyond the local subnet regardless of the Time to Live (TTL) value in the IP header. |
| 224.0.1.0 to 238.255.255.255 | Globally scoped group addresses. This block includes two types of designated group addresses:<br>• 232.0.0.0/8: SSM group addresses, and<br>• 233.0.0.0/8: Glop group addresses. |
| 239.0.0.0 to 239.255.255.255 | Administratively scoped multicast addresses. These addresses are considered to be locally rather than globally unique, and can be reused in domains administered by different organizations without causing conflicts. For details, refer to RFC 2365. |

**Note**

- The membership of a group is dynamic. Hosts can join or leave multicast groups at any time.
- "Glop" is a mechanism for assigning multicast addresses between different autonomous systems (ASs). By filling an AS number into the middle two bytes of 233.0.0.0, you get 255 multicast addresses for that AS. For more information, refer to RFC 2770.

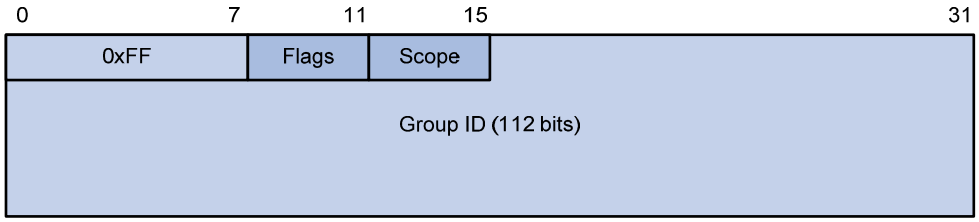
**Table 1-3** Some reserved multicast addresses

| Address | Description |
|---|---|
| 224.0.0.1 | All systems on this subnet, including hosts and routers |
| 224.0.0.2 | All multicast routers on this subnet |
| 224.0.0.3 | Unassigned |
| 224.0.0.4 | Distance Vector Multicast Routing Protocol (DVMRP) routers |
| 224.0.0.5 | Open Shortest Path First (OSPF) routers |
| 224.0.0.6 | OSPF designated routers/backup designated routers |

| Address | Description |
|---|---|
| 224.0.0.7 | Shared Tree (ST) routers |
| 224.0.0.8 | ST hosts |
| 224.0.0.9 | Routing Information Protocol version 2 (RIPv2) routers |
| 224.0.0.11 | Mobile agents |
| 224.0.0.12 | Dynamic Host Configuration Protocol (DHCP) server/relay agent |
| 224.0.0.13 | All Protocol Independent Multicast (PIM) routers |
| 224.0.0.14 | Resource Reservation Protocol (RSVP) encapsulation |
| 224.0.0.15 | All Core-Based Tree (CBT) routers |
| 224.0.0.16 | Designated Subnetwork Bandwidth Management (SBM) |
| 224.0.0.17 | All SBMs |
| 224.0.0.18 | Virtual Router Redundancy Protocol (VRRP) |

2) IPv6 multicast addresses

**Figure 1-4** IPv6 multicast format




Referring to Figure 1-4, the meanings of the fields of an IPv6 multicast address are as follows:

- 0xFF: The most significant 8 bits are 11111111, indicating that this address is an IPv6 multicast address.

**Figure 1-5** Format of the Flags field


- Flags: Referring to Figure 1-5, the following table describes the four bits of the Flags field.

**Table 1-4** Description on the bits of the Flags field

| Bit | Description |
|---|---|
| 0 | Reserved, set to 0 |
| R | • When set to 0, it indicates that this address is an IPv6 multicast address without an embedded RP address<br>• When set to 1, it indicates that this address is an IPv6 multicast address with an embedded RP address (The P and T bits must also be set to 1) |
| P | • When set to 0, it indicates that this address is an IPv6 multicast address not based on a unicast prefix<br>• When set to 1, it indicates that this address is an IPv6 multicast address based on a unicast prefix (the T bit must also be set to 1) |

| Bit | Description |
|---|---|
| T | • When set to 0, it indicates that this address is an IPv6 multicast address permanently-assigned by IANA<br>• When set to 1, it indicates that this address is a transient, or dynamically assigned IPv6 multicast address |

- Scope: 4 bits, indicating the scope of the IPv6 internetwork for which the multicast traffic is intended. Possible values of this field are given in Table 1-5.

**Table 1-5** Values of the Scope field

| Value | Meaning |
|---|---|
| 0, 3, F | Reserved |
| 1 | Interface-local scope |
| 2 | Link-local scope |
| 4 | Admin-local scope |
| 5 | Site-local scope |
| 6, 7, 9 through D | Unassigned |
| 8 | Organization-local scope |
| E | Global scope |

- Group ID: 112 bits, IPv6 multicast group identifier that uniquely identifies an IPv6 multicast group in the scope defined by the Scope field.

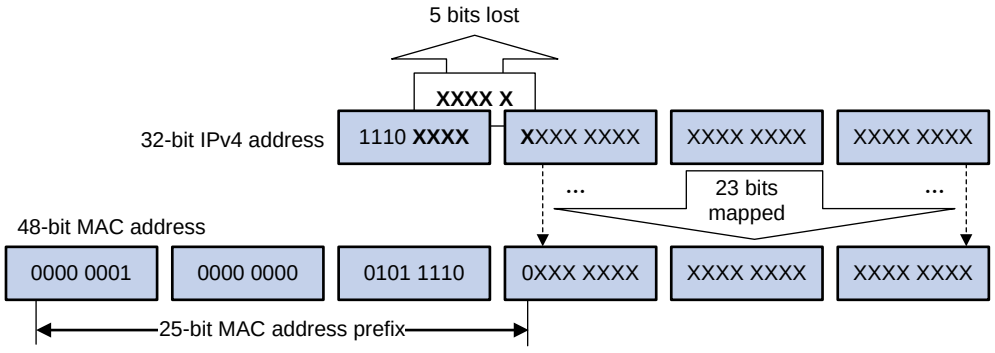
## Ethernet multicast MAC addresses

When a unicast IP packet is transmitted over Ethernet, the destination MAC address is the MAC address of the receiver. When a multicast packet is transmitted over Ethernet, however, the destination address is a multicast MAC address because the packet is directed to a group formed by a number of receivers, rather than to one specific receiver.

1) IPv4 multicast MAC addresses

As defined by IANA, the high-order 24 bits of an IPv4 multicast MAC address are 0x01005E, bit 25 is 0, and the low-order 23 bits are the low-order 23 bits of a multicast IPv4 address. The IPv4-to-MAC mapping relation is shown in Figure 1-6.

**Figure 1-6** IPv4-to-MAC address mapping

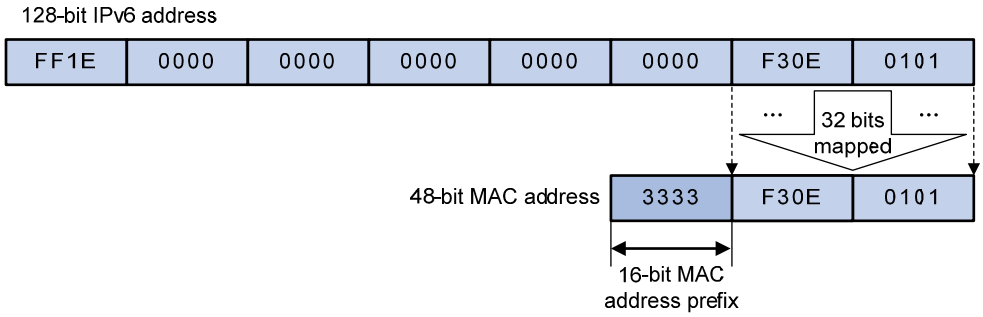


The high-order four bits of a multicast IPv4 address are 1110, indicating that this address is a multicast address, and only 23 bits of the remaining 28 bits are mapped to a MAC address, so five bits of the multicast IPv4 address are lost. As a result, 32 multicast IPv4 addresses map to the same MAC address. Therefore, in Layer 2 multicast forwarding, a device may receive some multicast data addressed for other IPv4 multicast groups, and such redundant data needs to be filtered by the upper layer.

2) IPv6 multicast MAC addresses

The high-order 16 bits of an IPv6 multicast MAC address are 0x3333, and the low-order 32 bits are the low-order 32 bits of a multicast IPv6 address. Figure 1-7 shows an example of mapping an IPv6 multicast address, FF1E::F30E:101, to a MAC address.

**Figure 1-7** An example of IPv6-to-MAC address mapping




## Multicast Protocols

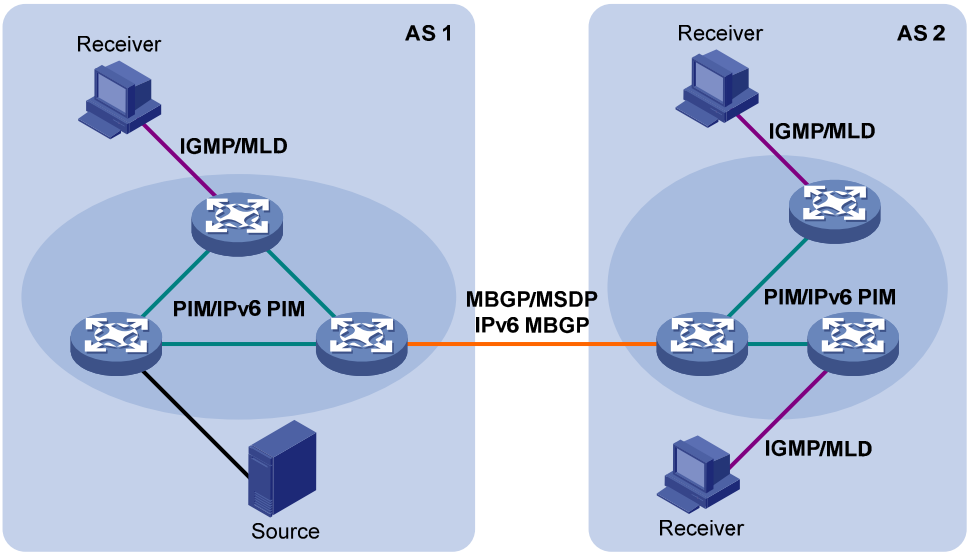
**Note**

- Generally, we refer to IP multicast working at the network layer as Layer 3 multicast and the corresponding multicast protocols as Layer 3 multicast protocols, which include IGMP/MLD, PIM/IPv6 PIM, MSDP, and MBGP/IPv6 MBGP; we refer to IP multicast working at the data link layer as Layer 2 multicast and the corresponding multicast protocols as Layer 2 multicast protocols, which include IGMP Snooping/MLD Snooping, and multicast VLAN/IPv6 multicast VLAN.
- IGMP Snooping, IGMP, multicast VLAN, PIM, MSDP, and MBGP are for IPv4, MLD Snooping, MLD, IPv6 multicast VLAN, IPv6 PIM, and IPv6 MBGP are for IPv6.
- This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network.

### Layer 3 multicast protocols

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols. Figure 1-8 describes where these multicast protocols are in a network.

**Figure 1-8** Positions of Layer 3 multicast protocols




1) Multicast management protocols

Typically, the internet group management protocol (IGMP) or multicast listener discovery protocol (MLD) is used between hosts and Layer 3 multicast devices directly connected with the hosts. These protocols define the mechanism of establishing and maintaining group memberships between hosts and Layer 3 multicast devices.

2) Multicast routing protocols

A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and forward multicast packets correctly and efficiently. Multicast routes constitute a loop-free data transmission path from a data source to multiple receivers, namely, a multicast distribution tree.

In the ASM model, multicast routes come in intra-domain routes and inter-domain routes.

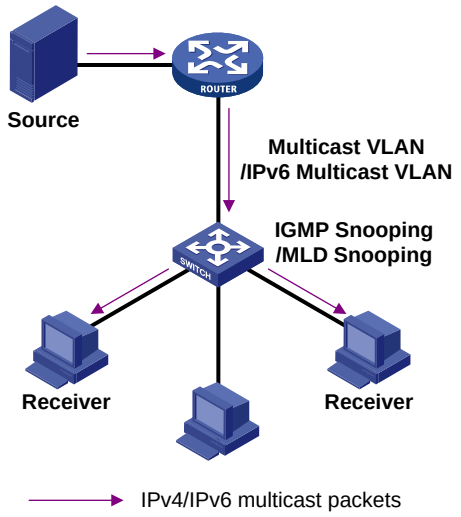
- An intra-domain multicast routing protocol is used to discover multicast sources and build multicast distribution trees within an AS so as to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, protocol independent multicast (PIM) is a popular one. Based on the forwarding mechanism, PIM comes in two modes – dense mode (often referred to as PIM-DM) and sparse mode (often referred to as PIM-SM).
- An inter-domain multicast routing protocol is used for delivery of multicast information between two ASs. So far, mature solutions include multicast source discovery protocol (MSDP) and multicast border gateway protocol (MBGP). MSDP is used to propagate multicast source information among different ASs, while MBGP, an extension of the Multi-protocol Border Gateway Protocol (MP-BGP), is used for exchanging multicast routing information among different ASs.

For the SSM model, multicast routes are not divided into inter-domain routes and intra-domain routes. Since receivers know the position of the multicast source, channels established through PIM-SM are sufficient for multicast information transport.

## Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP Snooping/MLD Snooping and multicast VLAN/IPv6 multicast VLAN. Figure 1-9 shows where these protocols are in the network.

**Figure 1-9** Position of Layer 2 multicast protocols




1) IGMP Snooping/MLD Snooping

Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) and Multicast Listener Discovery Snooping (MLD Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP or MLD messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling the flooding of multicast data in a Layer 2 network.

2) Multicast VLAN/IPv6 multicast VLAN

In the traditional multicast-on-demand mode, when users in different VLANs on a Layer 2 device need multicast information, the upstream Layer 3 device needs to forward a separate copy of the multicast data to each VLAN of the Layer 2 device. With the multicast VLAN or IPv6 multicast VLAN feature enabled on the Layer 2 device, the Layer 3 multicast device needs to send only one copy of multicast to the multicast VLAN or IPv6 multicast VLAN on the Layer 2 device. This avoids waste of network bandwidth and extra burden on the Layer 3 device.

## Multicast Packet Forwarding Mechanism

In a multicast model, a multicast source sends information to the host group identified by the multicast group address in the destination address field of IP multicast packets. Therefore, to deliver multicast packets to receivers located in different parts of the network, multicast routers on the forwarding path usually need to forward multicast packets received on one incoming interface to multiple outgoing interfaces. Compared with a unicast model, a multicast model is more complex in the following aspects.

- To ensure multicast packet transmission in the network, unicast routing tables or multicast routing tables (for example, the MBGP routing table) specially provided for multicast must be used as guidance for multicast forwarding.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet is subject to a reverse path forwarding (RPF) check on the incoming interface. The result of the RPF check determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

# Table of Contents

# 1 IGMP Snooping Configuration

When configuring IGMP Snooping, go to the following sections for information you are interested in:

- IGMP Snooping Overview
- IGMP Snooping Configuration Task List
- Displaying and Maintaining IGMP Snooping
- IGMP Snooping Configuration Examples
- Troubleshooting IGMP Snooping Configuration

## IGMP Snooping Overview

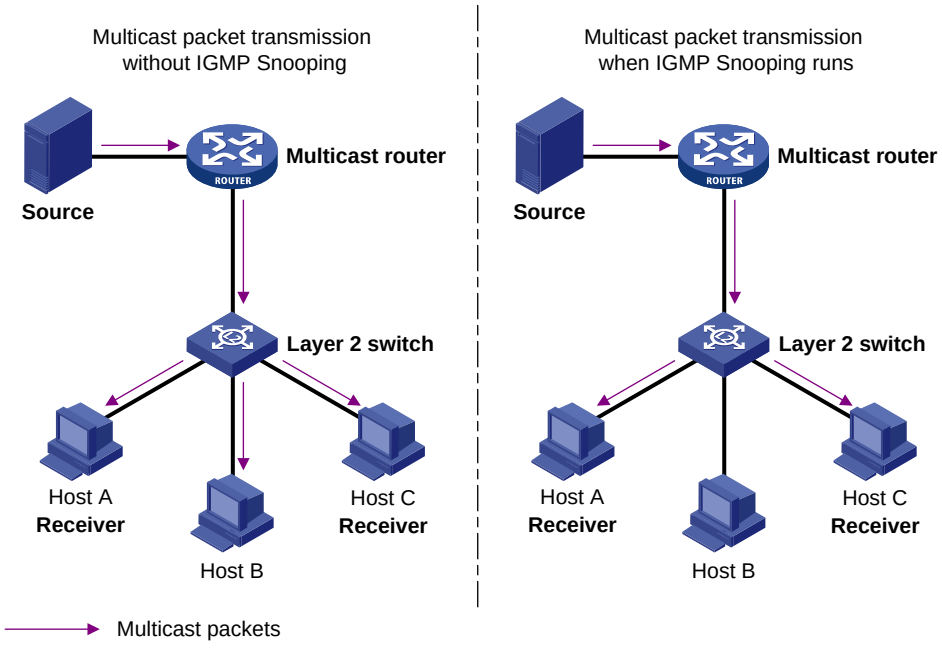
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

### Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in Figure 1-1, when IGMP Snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

**Figure 1-1** Before and after IGMP Snooping is enabled on the Layer 2 device




IGMP Snooping forwards multicast data to only the receivers requiring it at Layer 2. It brings the following advantages:

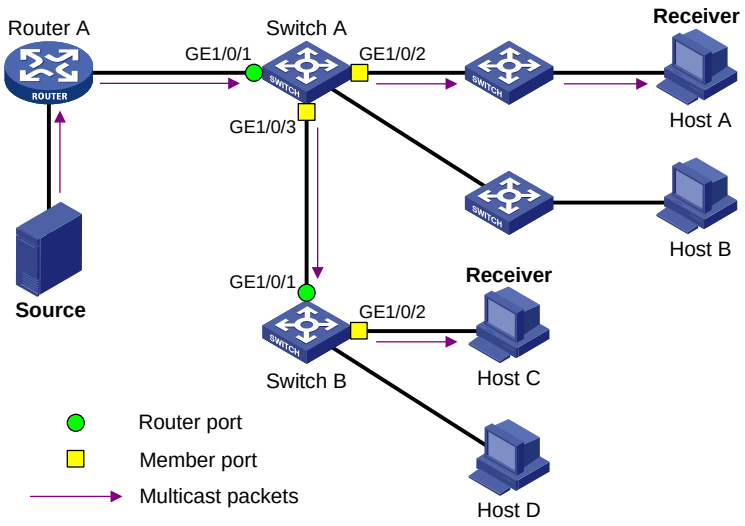
- Reducing Layer 2 broadcast packets, thus saving network bandwidth.
- Enhancing the security of multicast traffic.
- Facilitating the implementation of per-host accounting.

## Basic Concepts in IGMP Snooping

### IGMP Snooping related ports

As shown in Figure 1-2, Router A connects to the multicast source, IGMP Snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

**Figure 1-2** IGMP Snooping related ports




Ports involved in IGMP Snooping, as shown in Figure 1-2, are described as follows:

- Router port: A router port is a port on an Ethernet switch that leads switch towards a Layer 3 multicast device (DR or IGMP querier). In the figure, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. The switch registers all its local router ports in its router port list.
- Member port: A member port is a port on an Ethernet switch that leads the switch towards multicast group members. In the figure, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. The switch registers all the member ports on the local device in its IGMP Snooping forwarding table.

---

**Note**

- Whenever mentioned in this document, a router port is a port on the switch that leads the switch to a Layer 3 multicast device, rather than a port on a router.
- Unless otherwise specified, router/member ports mentioned in this document include static and dynamic ports.
- An IGMP-snooping-enabled switch deems that all its ports on which IGMP general queries with the source IP address other than 0.0.0.0 or PIM hello messages are received to be dynamic router ports.

---

### Aging timers for dynamic ports in IGMP Snooping and related messages and actions

**Table 1-1** Aging timers for dynamic ports in IGMP Snooping and related messages and actions

| Timer | Description | Message before expiry | Action after expiry |
|---|---|---|---|
| Dynamic router port aging timer | For each dynamic router port, the switch sets a timer initialized to the dynamic router port aging time. | IGMP general query of which the source address is not 0.0.0.0 or PIM hello | The switch removes this port from its router port list. |
| Dynamic member port aging timer | When a port dynamically joins a multicast group, the switch sets a timer for the port, which is initialized to the dynamic member port aging time. | IGMP membership report | The switch removes this port from the IGMP Snooping forwarding table. |

**Note**

The port aging mechanism of IGMP Snooping works only for dynamic ports; a static port will never age out.

## How IGMP Snooping Works

A switch running IGMP Snooping performs different actions when it receives different IGMP messages, as follows:

**Caution**

The description about adding or deleting a port in this section is only for a dynamic port. Static ports can be added or deleted only through the corresponding configurations. For details, see Configuring Static Ports.

### When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- If the receiving port is a dynamic router port existing in its router port list, the switch resets the aging timer of this dynamic router port.
- If the receiving port is not a dynamic router port existing in its router port list, the switch adds it into its router port list and sets an aging timer for this dynamic router port.

### When receiving a membership report

A host sends an IGMP report to the IGMP querier in the following circumstances:

- Upon receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When intended to join a multicast group, a host sends an IGMP report to the IGMP querier to announce that it is interested in the multicast information addressed to that group.

Upon receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group, and performs the following:

- If no forwarding table entry exists for the reported group, the switch creates an entry, adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported group, but the port is not included in the outgoing port list for that group, the switch adds the port as a dynamic member port to the outgoing port list, and starts an aging timer for that port.
- If a forwarding table entry exists for the reported group and the port is included in the outgoing port list, which means that this port is already a dynamic member port, the switch resets the aging timer for that port.

---

**Note**

A switch does not forward an IGMP report through a non-router port. The reason is as follows: Due to the IGMP report suppression mechanism, if the switch forwards a report message through a member port, all the attached hosts listening to the reported multicast address will suppress their own reports upon receiving this report, and this will prevent the switch from knowing whether the reported multicast group still has active members attached to that port.

---

### When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the dynamic member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router.

When the switch receives an IGMP leave message on a dynamic member port, the switch first checks whether a forwarding table entry for the group address in the message exists, and, if one exists, whether the outgoing port list contains the port.

- If the forwarding table entry does not exist or if the outgoing port list does not contain the port, the switch discards the IGMP leave message instead of forwarding it to any port.
- If the forwarding table entry exists and the outgoing port list contains the port, the switch forwards the leave message to all router ports in the native VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that group address, the switch does not immediately remove the port from the outgoing port list of the forwarding table entry for that group; instead, it resets the aging timer for the port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to that multicast group through the port that received the leave message. Upon receiving the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that multicast group, and performs the following to the port on which it received the IGMP leave message:

- If any IGMP report in response to the group-specific query is received on the port (suppose it is a dynamic member port) before its aging timer expires, this means that some host attached to the port is receiving or expecting to receive multicast data for that multicast group. The switch resets the aging timer of the port.
- If no IGMP report in response to the group-specific query is received on the port before its aging timer expires, this means that no hosts attached to the port are still listening to that group address: the switch removes the port from the outgoing port list of the forwarding table entry for that multicast group when the aging timer expires.

### Protocols and Standards

IGMP Snooping is documented in:

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

## IGMP Snooping Configuration Task List

Complete these tasks to configure IGMP Snooping:

| Task | | Remarks |
|---|---|---|
| Configuring Basic Functions of IGMP Snooping | Enabling IGMP Snooping | Required |
| | Configuring the Version of IGMP Snooping | Optional |
| Configuring IGMP Snooping Port Functions | Configuring Aging Timers for Dynamic Ports | Optional |
| | Configuring Static Ports | Optional |
| | Configuring Simulated Joining | Optional |
| | Configuring Fast Leave Processing | Optional |
| Configuring IGMP Snooping Querier | Enabling IGMP Snooping Querier | Optional |
| | Configuring IGMP Queries and Responses | Optional |
| | Configuring Source IP Address of IGMP Queries | Optional |
| Configuring an IGMP Snooping Policy | Configuring a Multicast Group Filter | Optional |
| | Configuring Multicast Source Port Filtering | Optional |
| | Configuring the Function of Dropping Unknown Multicast Data | Optional |
| | Configuring IGMP Report Suppression | Optional |
| | Configuring Maximum Multicast Groups that Can Be Joined on a Port | Optional |
| | Configuring Multicast Group Replacement | Optional |

**Note**

- Configurations made in IGMP Snooping view are effective for all VLANs, while configurations made in VLAN view are effective only for ports belonging to the current VLAN. For a given VLAN, a configuration made in IGMP Snooping view is effective only if the same configuration is not made in VLAN view.
- Configurations made in IGMP Snooping view are effective for all ports; configurations made in Ethernet port view are effective only for the current port; configurations made in Layer 2 aggregate port view are effect only for the current port; configurations made in port group view are effective only for all the ports in the current port group. For a given port, a configuration made in IGMP Snooping view is effective only if the same configuration is not made in Ethernet port view, Layer 2 aggregate port view or port group view.
- For IGMP Snooping, configurations made on a Layer 2 aggregate port do not interfere with configurations made on its member ports, nor do they take part in aggregation calculations; configurations made on a member port of the aggregate group will not take effect until it leaves the aggregate group.

# Configuring Basic Functions of IGMP Snooping

## Configuration Prerequisites

Before configuring the basic functions of IGMP Snooping, complete the following task:

- Configure the corresponding VLANs.

Before configuring the basic functions of IGMP Snooping, prepare the following data:

- Version of IGMP Snooping.

## Enabling IGMP Snooping

Follow these steps to enable IGMP Snooping:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IGMP Snooping globally and enter IGMP-Snooping view | **igmp-snooping** | Required<br>Disabled by default |
| Return to system view | **quit** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable IGMP Snooping in the VLAN | **igmp-snooping enable** | Required<br>Disabled by default |

**Note**

- IGMP Snooping must be enabled globally before it can be enabled in a VLAN.
- When you enable IGMP Snooping in a specified VLAN, this function takes effect for the ports in this VLAN only.

### Configuring the Version of IGMP Snooping

By configuring an IGMP Snooping version, you actually configure the version of IGMP messages that IGMP Snooping can process.

- IGMP Snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN.
- IGMP Snooping version 3 can process IGMPv1, IGMPv2 and IGMPv3 messages.

Follow these steps to configure the version of IGMP Snooping:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure the version of IGMP Snooping | **igmp-snooping version** *version-number* | Optional<br>Version 2 by default |

**Caution**

If you switch IGMP Snooping from version 3 to version 2, the system will clear all IGMP Snooping forwarding entries from dynamic joins, and will:

- Keep forwarding entries for version 3 static (*, G) joins;
- Clear forwarding entries from version 3 static (S, G) joins, which will be restored when IGMP Snooping is switched back to version 3.

For details about static joins, Refer to Configuring Static Ports.

## Configuring IGMP Snooping Port Functions

### Configuration Prerequisites

Before configuring IGMP Snooping port functions, complete the following tasks:

- Enable IGMP Snooping in the VLAN or enable IGMP on the VLAN interface
- Configure the corresponding port groups.

Before configuring IGMP Snooping port functions, prepare the following data:

- Aging time of dynamic router ports,
- Aging time of dynamic member ports, and
- Multicast group and multicast source addresses

## Configuring Aging Timers for Dynamic Ports

If the switch receives no IGMP general queries or PIM hello messages on a dynamic router port, the switch removes the port from the router port list when the aging timer of the port expires.

If the switch receives no IGMP reports for a multicast group on a dynamic member port, the switch removes the port from the outgoing port list of the forwarding table entry for that multicast group when the aging timer of the port for that group expires.

If multicast group memberships change frequently, you can set a relatively small value for the dynamic member port aging timer, and vice versa.

### Configuring aging timers for dynamic ports globally

Follow these steps to configure aging timers for dynamic ports globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Configure dynamic router port aging time | **router-aging-time** *interval* | Optional<br>105 seconds by default |
| Configure dynamic member port aging time | **host-aging-time** *interval* | Optional<br>260 seconds by default |

### Configuring aging timers for dynamic ports in a VLAN

Follow these steps to configure aging timers for dynamic ports in a VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure dynamic router port aging time | **igmp-snooping**<br>**router-aging-time** *interval* | Optional<br>105 seconds by default |
| Configure dynamic member port aging time | **igmp-snooping**<br>**host-aging-time** *interval* | Optional<br>260 seconds by default |

## Configuring Static Ports

If all the hosts attached to a port are interested in the multicast data addressed to a particular multicast group or the multicast data that a particular multicast source sends to a particular group, you can configure static (*, G) or (S, G) joining on that port, namely configure the port as a group-specific or source-and-group-specific static member port.

You can configure a port of a switch to be a static router port, through which the switch can forward all the multicast traffic it received.

Follow these steps to configure static ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure the port(s) as static member port(s) | **igmp-snooping static-group** *group-address* [ **source-ip** *source-address* ] **vlan** *vlan-id* | Required<br>No static member ports by default |
| Configure the port(s) as static router port(s) | **igmp-snooping static-router-port vlan** *vlan-id* | Required<br>No static router ports by default |

**Note**

- A static (S, G) joining can take effect only if a valid multicast source address is specified and IGMP Snooping version 3 is currently running.
- A static member port does not respond to queries from the IGMP querier; when static (*, G) or (S, G) joining is enabled or disabled on a port, the port does not send an unsolicited IGMP report or an IGMP leave message.
- Static member ports and static router ports never age out. To remove such a port, you need to use the corresponding **undo** command.

## Configuring Simulated Joining

Generally, a host running IGMP responds to IGMP queries from the IGMP querier. If a host fails to respond due to some reasons, the multicast router may deem that no member of this multicast group exists on the network segment, and therefore will remove the corresponding forwarding path.

To avoid this situation from happening, you can enable simulated joining on a port of the switch, namely configure the port as a simulated member host for a multicast group. When receiving an IGMP query, the simulated host gives a response. Thus, the switch can continue receiving multicast data.

A simulated host acts like a real host, as follows:

- When a port is configured as a simulated member host, the switch sends an unsolicited IGMP report through that port.
- After a port is configured as a simulated member host, the switch responds to IGMP general queries by sending IGMP reports through that port.
- When the simulated joining function is disabled on a port, the switch sends an IGMP leave message through that port.

Follow these steps to configure simulated joining:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure simulated (*, G) or (S, G) joining | **igmp-snooping host-join** *group-address* [ **source-ip** *source-address* ] **vlan** *vlan-id* | Required<br>Disabled by default |

**Note**

- Each simulated host is equivalent to an independent host. For example, when receiving an IGMP query, the simulated host corresponding to each configuration responds respectively.
- Unlike a static member port, a port configured as a simulated member host will age out like a dynamic member port.

## Configuring Fast Leave Processing

The fast leave processing feature allows the switch to process IGMP leave messages in a fast way. With the fast leave processing feature enabled, when receiving an IGMP leave message on a port, the switch immediately removes that port from the outgoing port list of the forwarding table entry for the indicated group. Then, when receiving IGMP group-specific queries for that multicast group, the switch will not forward them to that port.

In VLANs where only one host is attached to each port, fast leave processing helps improve bandwidth and resource usage.

### Configuring fast leave processing globally

Follow these steps to configure fast leave processing globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Enable fast leave processing | **fast-leave** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

### Configuring fast leave processing on a port or a group of ports

Follow these steps to configure fast leave processing on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable fast leave processing | **igmp-snooping fast-leave** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

**Caution**

If fast leave processing is enabled on a port to which more than one host is attached, when one host leaves a multicast group, the other hosts attached to the port and interested in the same multicast group will fail to receive multicast data for that group.

# Configuring IGMP Snooping Querier

## Configuration Prerequisites

Before configuring IGMP Snooping querier, complete the following task:

- Enable IGMP Snooping in the VLAN.

Before configuring IGMP Snooping querier, prepare the following data:

- IGMP general query interval,
- IGMP last-member query interval,
- Maximum response time to IGMP general queries,
- Source address of IGMP general queries, and
- Source address of IGMP group-specific queries.

## Enabling IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast switch is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as the IGMP Snooping querier to send IGMP queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Follow these steps to enable IGMP Snooping querier:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable IGMP Snooping querier | **igmp-snooping querier** | Required<br>Disabled by default |

**Caution**

It is meaningless to configure an IGMP Snooping querier in a multicast network running IGMP. Although an IGMP Snooping querier does not take part in IGMP querier elections, it may affect IGMP querier elections because it sends IGMP general queries with a low source IP address.

## Configuring IGMP Queries and Responses

You can tune the IGMP general query interval based on actual condition of the network.

Upon receiving an IGMP query (general query or group-specific query), a host starts a timer for each multicast group it has joined. This timer is initialized to a random value in the range of 0 to the maximum response time (the host obtains the value of the maximum response time from the Max Response Time field in the IGMP query it received). When the timer value comes down to 0, the host sends an IGMP report to the corresponding multicast group.

An appropriate setting of the maximum response time for IGMP queries allows hosts to respond to queries quickly and avoids bursts of IGMP traffic on the network caused by reports simultaneously sent by a large number of hosts when the corresponding timers expire simultaneously.

- For IGMP general queries, you can configure the maximum response time to fill their Max Response time field.
- For IGMP group-specific queries, you can configure the IGMP last-member query interval to fill their Max Response time field. Namely, for IGMP group-specific queries, the maximum response time equals to the IGMP last-member query interval.

### Configuring IGMP queries and responses globally

Follow these steps to configure IGMP queries and responses globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Configure the maximum response time to IGMP general queries | **max-response-time** *interval* | Optional<br>10 seconds by default |
| Configure the IGMP last-member query interval | **last-member-query-interval** *interval* | Optional<br>1 second by default |

### Configuring IGMP queries and responses in a VLAN

Follow these steps to configure IGMP queries and responses in a VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure IGMP general query interval | **igmp-snooping query-interval** *interval* | Optional<br>60 seconds by default |
| Configure the maximum response time to IGMP general queries | **igmp-snooping max-response-time** *interval* | Optional<br>10 seconds by default |
| Configure the IGMP last-member query interval | **igmp-snooping last-member-query-interval** *interval* | Optional<br>1 second by default |

**Caution**

In the configuration, make sure that the IGMP general query interval is larger than the maximum response time for IGMP general queries. Otherwise, multicast group members may be deleted by mistake.

## Configuring Source IP Address of IGMP Queries

Upon receiving an IGMP query whose source IP address is 0.0.0.0 on a port, the switch does not enlist that port as a dynamic router port. This may prevent multicast forwarding entries from being correctly created at the data link layer and cause multicast traffic forwarding failure in the end. When a Layer 2 device acts as an IGMP-Snooping querier, to avoid the aforesaid problem, you are commended to configure a non-all-zero IP address as the source IP address of IGMP queries.

Follow these steps to configure source IP address of IGMP queries:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure the source address of IGMP general queries | **igmp-snooping general-query source-ip** { **current-interface** \| *ip-address* } | Optional<br>0.0.0.0 by default |
| Configure the source IP address of IGMP group-specific queries | **igmp-snooping special-query source-ip** { **current-interface** \| *ip-address* } | Optional<br>0.0.0.0 by default |

**Caution**

The source address of IGMP query messages may affect IGMP querier selection within the segment.

# Configuring an IGMP Snooping Policy

## Configuration Prerequisites

Before configuring an IGMP Snooping policy, complete the following task:

- Enable IGMP Snooping in the VLAN or enable IGMP on the desired VLAN interface

Before configuring an IGMP Snooping policy, prepare the following data:

- ACL rule for multicast group filtering
- The maximum number of multicast groups that can pass the ports

## Configuring a Multicast Group Filter

On an IGMP Snooping–enabled switch, the configuration of a multicast group allows the service provider to define restrictions on multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an IGMP report. Upon receiving this report message, the switch checks the report against the configured ACL rule. If the port on which the report was received can join this multicast group, the switch adds an entry for this port in the IGMP Snooping forwarding table; otherwise the switch drops this report message. Any multicast data that has failed the ACL check will not be sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

### Configuring a multicast group filter globally

Follow these steps to configure a multicast group filter globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Configure a multicast group filter | **group-policy** *acl-number* [ **vlan** *vlan-list* ] | Required<br>No group filter is configured by default. |

### Configuring a multicast group filter on a port or a group of ports

Follow these steps to configure a multicast group filter on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure a multicast group filter | **igmp-snooping group-policy** *acl-number* [ **vlan** *vlan-list* ] | Required<br>No group filter is configured by default. |

## Configuring Multicast Source Port Filtering

With the multicast source port filtering feature enabled on a port, the port can be connected with multicast receivers only rather than with multicast sources, because the port will block all multicast data packets while it permits multicast protocol packets to pass.

If this feature is disabled on a port, the port can be connected with both multicast sources and multicast receivers.

### Configuring multicast source port filtering globally

Follow these steps to configure multicast source port filtering globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Enable multicast source port filtering | **source-deny port** *interface-list* | Required<br>Disabled by default |

### Configuring multicast source port filtering on a port or a group of ports

Follow these steps to configure multicast source port filtering on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable multicast source port filtering | **igmp-snooping source-deny** | Required<br>Disabled by default |

**Note**

3Com Switch 4500G, when enabled to filter IPv4 multicast data based on the source ports, are automatically enabled to filter IPv6 multicast data based on the source ports.

## Configuring the Function of Dropping Unknown Multicast Data

Unknown multicast data refers to multicast data for which no entries exist in the IGMP Snooping forwarding table. When receiving such multicast traffic, the switch floods it in the VLAN, incurring network bandwidth waste and low forwarding efficiency.

With the function of dropping unknown multicast data enabled, the switch forwards unknown multicast data to its router ports instead of flooding it in the VLAN. If no router ports exist, the switch drops the unknown multicast data..

Follow these steps to configure the function of dropping unknown multicast data in a VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable the function of dropping unknown multicast data | **igmp-snooping drop-unknown** | Required<br>Disabled by default |

## Configuring IGMP Report Suppression

When a Layer 2 device receives an IGMP report from a multicast group member, the device forwards the message to the Layer 3 device directly connected with it. Thus, when multiple members of a multicast group are attached to the Layer 2 device, the Layer 3 device directly connected with it will receive duplicate IGMP reports from these members.

With the IGMP report suppression function enabled, within each query cycle, the Layer 2 device forwards only the first IGMP report per multicast group to the Layer 3 device and will not forward the subsequent IGMP reports from the same multicast group to the Layer 3 device. This helps reduce the number of packets being transmitted over the network.

Follow these steps to configure IGMP report suppression:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Enable IGMP report suppression | **report-aggregation** | Optional<br>Enabled by default |

## Configuring Maximum Multicast Groups that Can Be Joined on a Port

By configuring the maximum number of multicast groups that can be joined on a port, you can limit the number of multicast programs on-demand available to users, thus to regulate traffic on the port.

Follow these steps to configure the maximum number of multicast groups allowed on a port or ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure the maximum number of multicast groups allowed on the port(s) | **igmp-snooping group-limit** *limit* [ **vlan** *vlan-list* ] | Optional<br>By default, the maximum number of multicast groups allowed on the port(s) is 128. |

**Note**

- When the number of multicast groups a port has joined reaches the maximum number configured, the system deletes all the forwarding entries persistent to that port from the IGMP Snooping forwarding table, and the hosts on this port need to join the multicast groups again.
- If you have configured static or simulated joins on a port, however, when the number of multicast groups on the port exceeds the configured threshold, the system deletes all the forwarding entries persistent to that port from the IGMP Snooping forwarding table and applies the static or simulated joins again, until the number of multicast groups joined by the port comes back within the configured threshold.

## Configuring Multicast Group Replacement

For some special reasons, the number of multicast groups that can be joined on the current switch or port may exceed the number configured for the switch or the port. In addition, in some specific applications, a multicast group newly joined on the switch needs to replace an existing multicast group automatically. A typical example is “channel switching”, namely, by joining a new multicast group, a user automatically switches from the current multicast group to the new one.

To address such situations, you can enable the multicast group replacement function on the switch or certain ports. When the number of multicast groups joined on the switch or a port has joined reaches the limit:

- If the multicast group replacement feature is enabled, the newly joined multicast group automatically replaces an existing multicast group with the lowest address.
- If the multicast group replacement feature is not enabled, new IGMP reports will be automatically discarded.

### Configuring multicast group replacement globally

Follow these steps to configure multicast group replacement globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter IGMP Snooping view | **igmp-snooping** | — |
| Enable multicast group replacement | **overflow-replace** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

### Configuring multicast group replacement on a port or a group of ports

Follow these steps to configure multicast group replacement on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable multicast group replacement | **igmp-snooping overflow-replace** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

**Caution**

Be sure to configure the maximum number of multicast groups allowed on a port (refer to Configuring Maximum Multicast Groups that Can Be Joined on a Port) before enabling multicast group replacement. Otherwise, the multicast group replacement functionality will not take effect.

## Displaying and Maintaining IGMP Snooping

| To do... | Use the command... | Remarks |
|---|---|---|
| View IGMP Snooping multicast group information | **display igmp-snooping group** [ **vlan** *vlan-id* ] [ **verbose** ] | Available in any view |
| View the statistics information of IGMP messages learned by IGMP Snooping | **display igmp-snooping statistics** | Available in any view |
| Clear IGMP Snooping multicast group information | **reset igmp-snooping group** { *group-address* \| **all** } [ **vlan** *vlan-id* ] | Available in user view |
| Clear the statistics information of all kinds of IGMP messages learned by IGMP Snooping | **reset igmp-snooping statistics** | Available in user view |

**Note**

- The **reset igmp-snooping group** command works only on an IGMP Snooping–enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.
- The **reset igmp-snooping group** command cannot clear the IGMP Snooping multicast group information for static joins.

# IGMP Snooping Configuration Examples

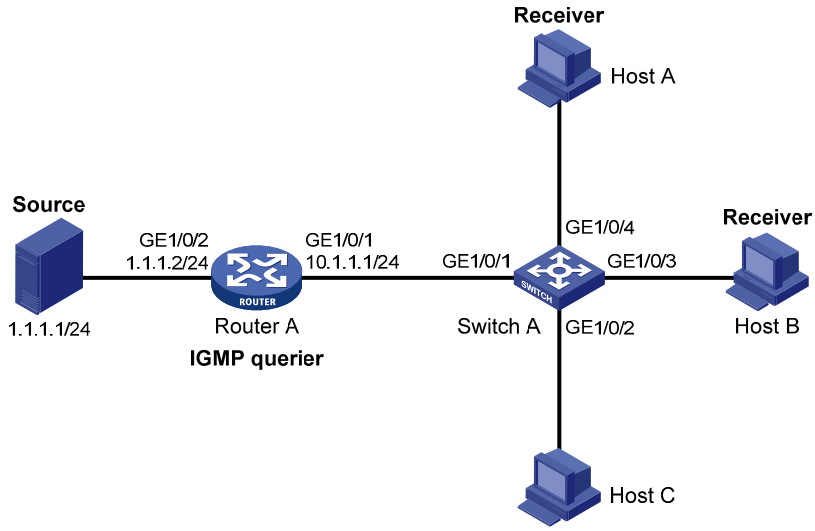
## Configuring Group Policy and Simulated Joining

### Network requirements

- As shown in Figure 1-3, Router A connects to the multicast source through GigabitEthernet 1/0/2 and to Switch A through GigabitEthernet 1/0/1.
- IGMPv2 is required on Router A, IGMP Snooping version 2 is required on Switch A, and Router A will act as the IGMP querier on the subnet.
- It is required that the receivers, Host A and Host B, attached to Switch A can receive multicast traffic addressed to multicast group 224.1.1.1 only.
- It is required that multicast data for group 224.1.1.1 can be forwarded through GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A even if Host A and Host B accidentally, temporarily stop receiving multicast data.

### Network diagram

**Figure 1-3** Network diagram for group policy simulated joining configuration




### Configuration procedure

1) Configure IP addresses

Configure an IP address and subnet mask for each interface as per Figure 1-3. The detailed configuration steps are omitted.

2) Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP Snooping and the function of dropping unknown multicast traffic in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

# Configure a multicast group filter so that the hosts in VLAN 100 can join only the multicast group 224.1.1.1.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated hosts for multicast group 224.1.1.1.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

4) Verify the configuration

# View the detailed IGMP Snooping multicast groups information in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1               (D) ( 00:01:30 )
```

```
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Attribute:    Host Port
      Host port(s):total 2 port.
        GE1/0/3                (D) ( 00:03:23 )
        GE1/0/4                (D) ( 00:04:10 )
MAC group(s):
  MAC group address:0100-5e01-0101
      Host port(s):total 2 port.
        GE1/0/3
        GE1/0/4
```

As shown above, GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A has joined multicast group 224.1.1.1.

## Static Port Configuration

### Network requirements

- As shown in Figure 1-4, Router A connects to a multicast source (Source) through GigabitEthernet 1/0/2, and to Switch A through GigabitEthernet 1/0/1.
- IGMPv2 is to run on Router A, and IGMPv2 Snooping is to run on Switch A, Switch B and Switch C, with Router A acting as the IGMP querier.
- Host A and host C are permanent receivers of multicast group 224.1.1.1. GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C are required to be configured as static member ports for multicast group 224.1.1.1 to enhance the reliability of multicast traffic transmission.
- Suppose STP runs on the network. To avoid data loops, the forwarding path from Switch A to Switch C is blocked under normal conditions, and multicast traffic flows to the receivers attached to Switch C only along the path of Switch A—Switch B—Switch C.
- It is required to configure GigabitEthernet 1/0/3 that connects Switch A to Switch C as a static router port, so that multicast traffic can flow to the receivers nearly uninterruptedly along the path of Switch A—Switch C in the case that the path of Switch A—Switch B—Switch C gets blocked.

---

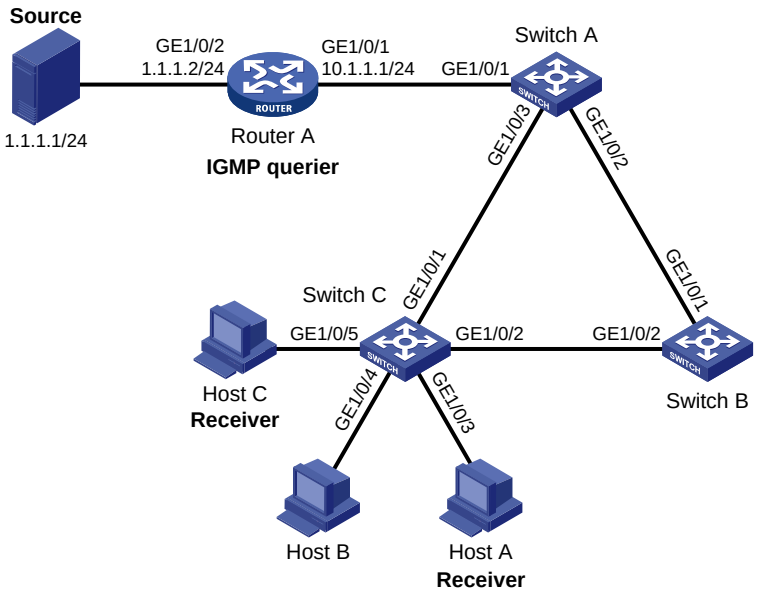
**Note**

If no static router port is configured, when the path of Switch A—Switch B—Switch C gets blocked, at least one IGMP query-response cycle must be completed before the multicast data can flow to the receivers along the new path of Switch A—Switch C, namely multicast delivery will be interrupted during this process.

---

## Network diagram

**Figure 1-4** Network diagram for static port configuration




## Configuration procedure

1) Configure IP addresses

Configure an IP address and subnet mask for each interface as per Figure 1-4. The detailed configuration steps are omitted.

2) Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchA-vlan100] igmp-snooping enable
```

```
[SwitchA-vlan100] quit
```

# Configure GigabitEthernet 1/0/3 to be a static router port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4) Configure Switch B

# Enable IGMP Snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

5) Configure Switch C

# Enable IGMP Snooping globally.

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for multicast group 224.1.1.1.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface GigabitEthernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

6) Verify the configuration

# View the detailed IGMP Snooping multicast group information in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 2 port.
            GE1/0/1               (D) ( 00:01:30 )
            GE1/0/3               (S)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 1 port.
            GE1/0/2               (D) ( 00:03:23 )
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/2
```

As shown above, GigabitEthernet 1/0/3 of Switch A has become a static router port.

# View the detailed IGMP Snooping multicast group information in VLAN 100 on Switch C.

```
[SwitchC] display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/2               (D) ( 00:01:23 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 2 port.
            GE1/0/3               (S)
            GE1/0/5               (S)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 2 port.
            GE1/0/3
            GE1/0/5
```

As shown above, GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for multicast group 224.1.1.1.

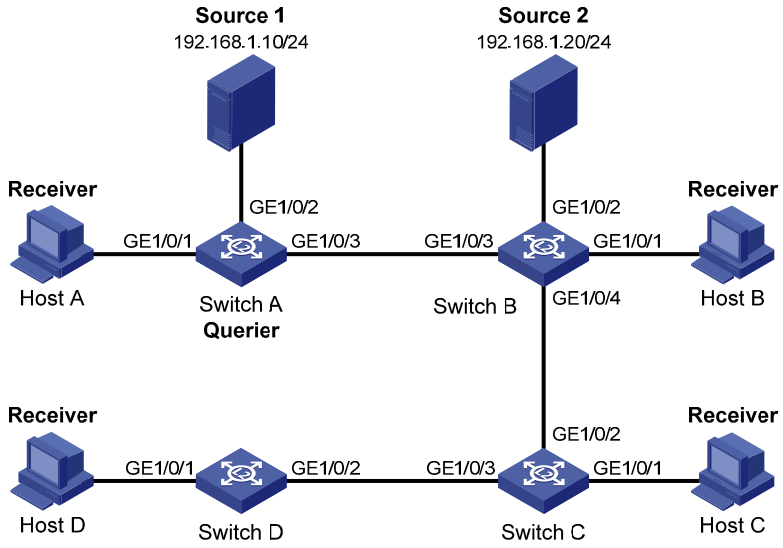
# IGMP Snooping Querier Configuration

## Network requirements

- As shown in Figure 1-5, in a Layer 2–only network environment, two multicast sources Source 1 and Source 2 send multicast data to multicast groups 224.1.1.1 and 225.1.1.1 respectively, Host A and Host C are receivers of multicast group 224.1.1.1, while Host B and Host D are receivers of multicast group 225.1.1.1.
- All the receivers are running IGMPv2, and all the switches need to run IGMP Snooping version 2. Switch A, which is close to the multicast sources, is chosen as the IGMP-Snooping querier.
- To prevent flooding of unknown multicast traffic within the VLAN, it is required to configure all the switches to drop unknown multicast data packets.
- Because a switch does not enlist a port that has heard an IGMP query with a source IP address of 0.0.0.0 (default) as a dynamic router port, configure a non-all-zero IP address as the source IP address of IGMP queries to ensure normal creation of Layer 2 multicast forwarding entries.

## Network diagram

**Figure 1-5** Network diagram for IGMP Snooping querier configuration




## Configuration procedure

1) Configure switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

# Enable IGMP Snooping and the function of dropping unknown multicast traffic in VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
```

# Enable the IGMP-Snooping querier function in VLAN 100

```
[SwitchA-vlan100] igmp-snooping querier
```

# Set the source IP address of IGMP general queries and group-specific queries to 192.168.1.1 in VLAN 100.

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

2) Configure Switch B

# Enable IGMP Snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable IGMP Snooping and the function of dropping unknown multicast traffic in VLAN 100.

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

Configurations on Switch C and Switch D are similar to the configuration on Switch B.

3) Verify the configuration

After the IGMP Snooping querier starts to work, all the switches but the querier can receive IGMP general queries. By using the **display igmp-snooping statistics** command, you can view the statistics information about the IGMP messages received. For example:

# View the IGMP message statistics on Switch B.

```
[SwitchB] display igmp-snooping statistics
  Received IGMP general queries:3.
  Received IGMPv1 reports:0.
  Received IGMPv2 reports:12.
  Received IGMP leaves:0.
  Received IGMPv2 specific queries:0.
  Sent     IGMPv2 specific queries:0.
  Received IGMPv3 reports:0.
  Received IGMPv3 reports with right and wrong records:0.
  Received IGMPv3 specific queries:0.
  Received IGMPv3 specific sg queries:0.
  Sent     IGMPv3 specific queries:0.
  Sent     IGMPv3 specific sg queries:0.
  Received error IGMP messages:0.
```

# Troubleshooting IGMP Snooping Configuration

## Switch Fails in Layer 2 Multicast Forwarding

### Symptom

A switch fails to implement Layer 2 multicast forwarding.

### Analysis

IGMP Snooping is not enabled.

### Solution

1) Enter the **display current-configuration** command to view the running status of IGMP Snooping.
2) If IGMP Snooping is not enabled, use the **igmp-snooping** command to enable IGMP Snooping globally, and then use **igmp-snooping enable** command to enable IGMP Snooping in VLAN view.
3) If IGMP Snooping is disabled only for the corresponding VLAN, just use the **igmp-snooping enable** command in VLAN view to enable IGMP Snooping in the corresponding VLAN.

## Configured Multicast Group Policy Fails to Take Effect

### Symptom

Although a multicast group policy has been configured to allow hosts to join specific multicast groups, the hosts can still receive multicast data addressed to other multicast groups.

### Analysis

- The ACL rule is incorrectly configured.
- The multicast group policy is not correctly applied.
- The function of dropping unknown multicast data is not enabled, so unknown multicast data is flooded.

### Solution

1) Use the **display acl** command to check the configured ACL rule. Make sure that the ACL rule conforms to the multicast group policy to be implemented.
2) Use the **display this** command in IGMP Snooping view or in the corresponding port view to check whether the correct multicast group policy has been applied. If not, use the **group-policy** or **igmp-snooping group-policy** command to apply the correct multicast group policy.
3) Use the **display current-configuration** command to check whether the function of dropping unknown multicast data is enabled. If not, use the **igmp-snooping drop-unknown** command to enable the function of dropping unknown multicast data.

# Table of Contents

# 1 Multicast VLAN Configuration

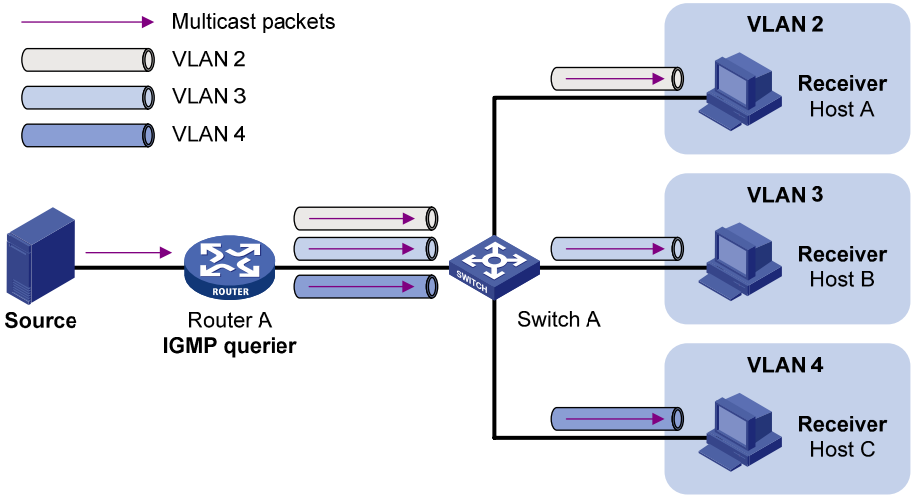
When configuring multicast VLAN, go to these sections for information you are interested in:



## Introduction to Multicast VLAN

As shown in Figure 1-1, in the traditional multicast programs-on-demand mode, when hosts, Host A, Host B and Host C, belonging to different VLANs require multicast programs on demand service, the Layer 3 device, Router A, needs to forward a separate copy of the multicast traffic in each user VLAN to the Layer 2 device, Switch A. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

**Figure 1-1** Multicast transmission without multicast VLAN



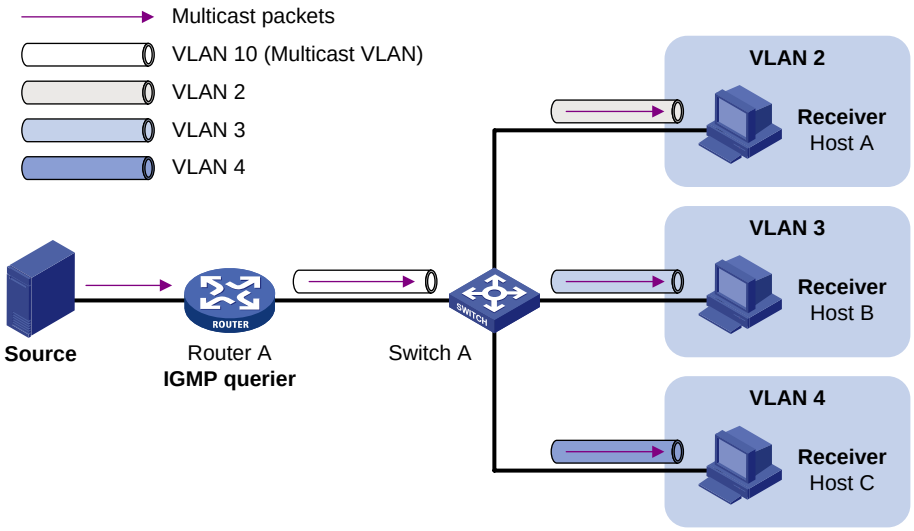

The multicast VLAN feature configured on the Layer 2 device is the solution to this issue. With the multicast VLAN feature, the Layer 3 device needs to replicate the multicast traffic only in the multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This saves the network bandwidth and lessens the burden of the Layer 3 device.

The multicast VLAN feature can be implemented in two approaches, as described below:

### Sub-VLAN-based multicast VLAN

As shown in Figure 1-2, Host A, Host B and Host C are in three different user VLANs. On Switch A, configure VLAN 10 as a multicast VLAN, configure all the user VLANs as sub-VLANs of this multicast VLAN, and enable IGMP Snooping in the multicast VLAN.

**Figure 1-2** Sub-VLAN-based multicast VLAN

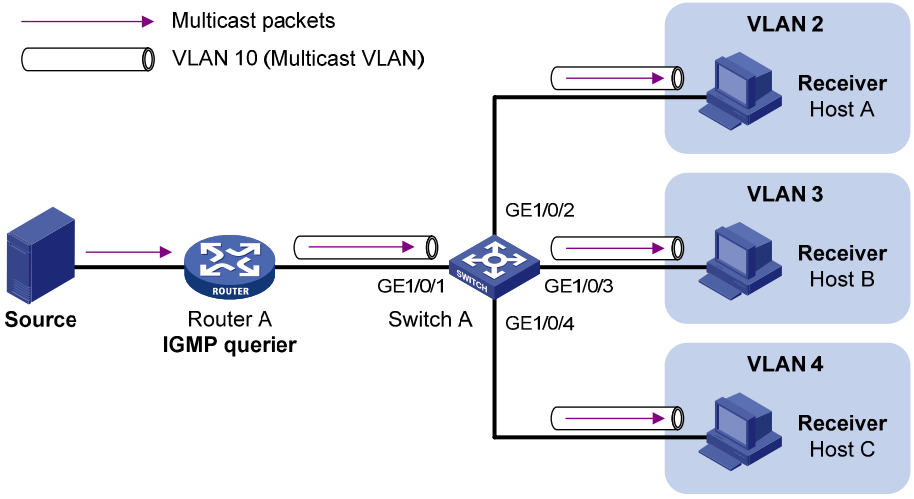



After the configuration, IGMP Snooping manages router ports in the multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the multicast VLAN, and Switch A distributes the traffic to the multicast VLAN's sub-VLANs that contain receivers.

## Port-based multicast VLAN

As shown in Figure 1-3, Host A, Host B and Host C are in three different user VLANs. All the user ports (ports with attached hosts) on Switch A are hybrid ports. On Switch A, configure VLAN 10 as a multicast VLAN, assign all the user ports to this multicast VLAN, and enable IGMP Snooping in the multicast VLAN and all the user VLANs.

**Figure 1-3** Port-based multicast VLAN




After the configuration, upon receiving an IGMP message on a user port, Switch A tags the message with the multicast VLAN ID and relays it to the IGMP querier, so that IGMP Snooping can uniformly manage the router ports and member ports in the multicast VLAN. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the multicast VLAN, and Switch A distributes the traffic to all the member ports in the multicast VLAN.

**Note**

- For information about IGMP Snooping, router ports, and member ports, refer to *IGMP Snooping Configuration* in the *IP Multicast Volume*.
- For information about VLAN tags, refer to *VLAN Configuration* in the *Access Volume*.

# Multicast VLAN Configuration Task List

Complete the following tasks to configure multicast VLAN:

| Task | | Remarks |
|---|---|---|
| Configuring Sub-VLAN-Based Multicast VLAN | | Required<br>Use either approach. |
| Configuring Port-Based Multicast VLAN | Configuring User Port Attributes | |
| | Configuring Multicast VLAN Ports | |

**Note**

If you have configured both sub-VLAN-based multicast VLAN and port-based multicast VLAN on a device, the port-based multicast VLAN configuration is given preference.

# Configuring Sub-VLAN-Based Multicast VLAN

## Configuration Prerequisites

Before configuring sub-VLAN-based multicast VLAN, complete the following tasks:

- Create VLANs as required
- Enable IGMP Snooping in the VLAN to be configured as a multicast VLAN

## Configuring Sub-VLAN-Based Multicast VLAN

In this approach, you need to configure a VLAN as a multicast VLAN, and then configure user VLANs as sub-VLANs of the multicast VLAN.

Follow these steps to configure sub-VLAN-based multicast VLAN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view | **multicast-vlan** *vlan-id* | Required<br>Not a multicast VLAN by default |
| Configure the specified VLAN(s) as sub-VLAN(s) of the multicast VLAN | **subvlan** *vlan-list* | Required<br>By default, a multicast VLAN has no sub-VLANs. |

Note

- The VLAN to be configured as a multicast VLAN must exist.
- The VLANs to be configured as sub-VLANs of the multicast VLAN must exist and must not be sub-VLANs of another multicast VLAN.
- The total number of sub-VLANs of a multicast VLAN must not exceed 63.

# Configuring Port-Based Multicast VLAN

When configuring port-based multicast VLAN, you need to configure the attributes of each user port and then assign the ports to the multicast VLAN.

Note

- A user port can be configured as a multicast VLAN port only if it is of the Ethernet or Layer 2 aggregate port type.
- Configurations made in Ethernet port view are effective only for the current port; configurations made in Layer 2 aggregate port view are effective only for the current port; configurations made in port group view are effective for all the ports in the current port group.

## Configuration Prerequisites

Before configuring port-based multicast VLAN, complete the following tasks:

- Create VLANs as required
- Enable IGMP Snooping in the VLAN to be configured as a multicast VLAN
- Enable IGMP Snooping in all the user VLANs

## Configuring User Port Attributes

Configure the user ports as hybrid ports that permit packets of the specified user VLAN to pass, and configure the user VLAN to which the user ports belong as the default VLAN.

Configure the user ports to permit packets of the multicast VLAN to pass and untag the packets. Thus, upon receiving multicast packets tagged with the multicast VLAN ID from the upstream device, the Layer 2 device untags the multicast packets and forwards them to its downstream device.

Follow these steps to configure user port attributes:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either command |
| | **port-group** { **manual** *port-group-name* \| **aggregation** *agg-id* } | |
| Configure the user port link type as hybrid | **port link-type hybrid** | Required<br>Access by default |
| Specify the user VLAN that comprises the current user port(s) as the default VLAN | **port hybrid pvid vlan** *vlan-id* | Required<br>VLAN 1 by default |
| Configure the current user port(s) to permit packets of the specified multicast VLAN(s) to pass and untag the packets | **port hybrid vlan** *vlan-id-list* **untagged** | Required<br>By default, a hybrid port permits only packets of VLAN 1 to pass. |

**Note**

For details about the **port link-type**, **port hybrid pvid vlan**, and **port hybrid vlan** commands, refer to *VLAN Commands* in the *Access Volume*.

## Configuring Multicast VLAN Ports

In this approach, you need to configure a VLAN as a multicast VLAN and then assign user ports to this multicast VLAN by either adding the user ports in the multicast VLAN or specifying the multicast VLAN on the user ports. These two configuration methods give the same result.

### Configuring multicast VLAN ports in multicast VLAN view

Follow these steps to configure multicast VLAN ports in multicast VLAN view:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view | **multicast-vlan** *vlan-id* | Required<br>Not a multicast VLAN by default |
| Assign ports to the multicast VLAN | **port** *interface-list* | Required<br>By default, a multicast VLAN has no ports. |

### Configuring multicast VLAN ports in port view or port group view

Follow these steps to configure multicast VLAN ports in port view or port group view:

| To do… | Use this command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view | **multicast-vlan** *vlan-id* | Required<br>Not a multicast VLAN by default. |
| Return to system view | **quit** | — |
| Enter port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either command. |
| | **port-group manual** *port-group-name* | |
| Configure the current port(s) as port(s) of the multicast VLAN | **port multicast-vlan** *vlan-id* | Required<br>By default, a user port does not belong to any multicast VLAN. |

**Note**

- The VLAN to be configured as a multicast VLAN must exist.
- A port can belong to only one multicast VLAN.

# Displaying and Maintaining Multicast VLAN

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about a multicast VLAN | **display multicast-vlan** [ *vlan-id* ] | Available in any view |

# Multicast VLAN Configuration Examples

## Sub-VLAN-Based Multicast VLAN Configuration

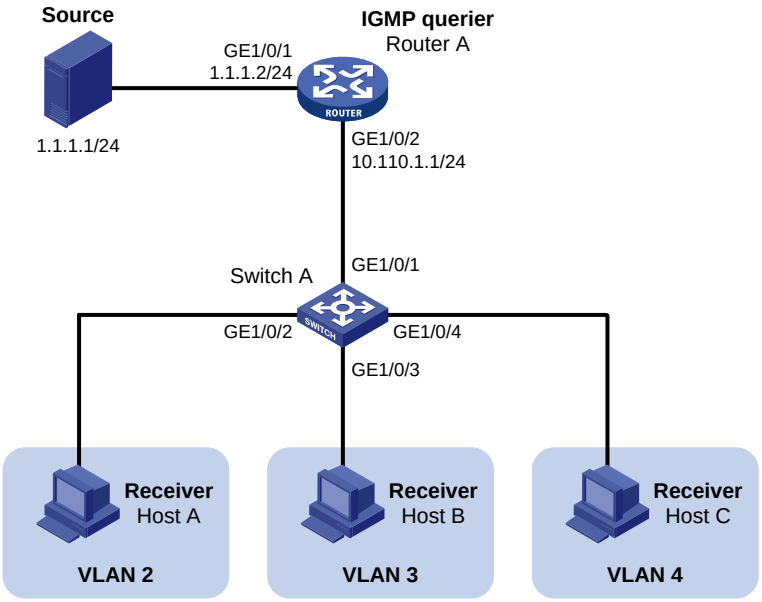
### Network requirements

- Router A connects to a multicast source through GigabitEthernet1/0/1 and to Switch A, through GigabitEthernet 1/0/2.
- IGMPv2 is required on Router A, and IGMPv2 Snooping is required on Switch A. Router A is the IGMP querier.
- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 of Switch A respectively.
- The multicast source sends multicast data to multicast group 224.1.1.1. Host A, Host B, and Host C are receivers of the multicast group.

- Configure the sub-VLAN-based multicast VLAN feature so that Router A just sends multicast data to Switch A through the multicast VLAN and Switch A forwards the traffic to the receivers that belong to different user VLANs.

## Network diagram

**Figure 1-4** Network diagram for sub-VLAN-based multicast VLAN configuration




## Configuration procedure

1) Configure IP addresses

Configure an IP address and subnet mask for each interface as per Figure 1-4. The detailed configuration steps are omitted here.

2) Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface and enable IGMP on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] igmp enable
```

3) Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 2 and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchA] vlan 2
```

```
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar to the configuration for VLAN 2.

# Create VLAN 10, assign GigabitEthernet 1/0/1 to this VLAN and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
```

# Configure VLAN 10 as a multicast VLAN and configure VLAN 2 through VLAN 4 as its sub-VLANs.

```
[SwitchA] multicast-vlan 10
[SwitchA-mvlan-10] subvlan 2 to 4
[SwitchA-mvlan-10] quit
```

4) Verify the configuration

# Display information about the multicast VLAN.

```
[SwitchA] display multicast-vlan
 Total 1 multicast-vlan(s)

 Multicast vlan 10
   subvlan list:
    vlan 2-4
   port list:
    no port
```

# View the IGMP Snooping multicast group information on Switch A.

```
[SwitchA] display igmp-snooping group
  Total 4 IP Group(s).
  Total 4 IP Source(s).
  Total 4 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port.
            GE1/0/2                (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            GE1/0/2

  Vlan(id):3.
```

```
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port.
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Host port(s):total 1 port.
          GE1/0/3               (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 1 port.
          GE1/0/3

Vlan(id):4.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port.
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Host port(s):total 1 port.
          GE1/0/4               (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 1 port.
          GE1/0/4

Vlan(id):10.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
          GE1/0/1               (D)
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Host port(s):total 0 port.
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 0 port.
```

As shown above, IGMP Snooping is maintaining the router port in the multicast VLAN (VLAN 10) and the member ports in the sub-VLANs (VLAN 2 through VLAN 4).

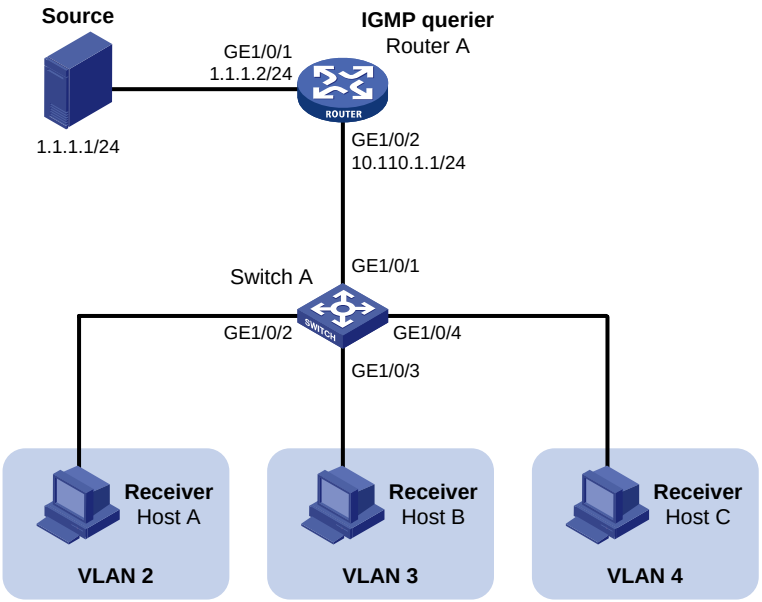
# Port-Based Multicast VLAN Configuration

## Network requirements

- As shown in Figure 1-5, Router A connects to a multicast source (Source) through GigabitEthernet 1/0/1, and to Switch A through GigabitEthernet 1/0/2.
- IGMPv2 is required on Router A. IGMPv2 Snooping is required on Switch A. Router A acts as the IGMP querier.
- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet1/0/4 of Switch A respectively.
- The multicast source sends multicast data to multicast group 224.1.1.1. Host A, Host B, and Host C are receivers of the multicast group.
- Configure the port-based multicast VLAN feature so that Router A just sends multicast data to Switch A through the multicast VLAN and Switch A forwards the multicast data to the receivers that belong to different user VLANs.

## Network diagram

**Figure 1-5** Network diagram for port-based multicast VLAN configuration




## Configuration procedure

1) Configure IP addresses

Configure the IP address and subnet mask for each interface as per Figure 1-5. The detailed configuration steps are omitted here.

2) Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
```

```
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] igmp enable
```

3) Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 10, assign GigabitEthernet 1/0/1 to VLAN 10, and enable IGMP Snooping in this VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
```

# Create VLAN 2 and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar. The detailed configuration steps are omitted.

# Configure GigabitEthernet 1/0/2 as a hybrid port. Configure VLAN 2 as the default VLAN. Configure GigabitEthernet 1/0/2 to permit packets of VLAN 2 and VLAN 10 to pass and untag the packets when forwarding them.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

The configuration for GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 is similar. The detailed configuration steps are omitted.

# Configure VLAN 10 as a multicast VLAN.

```
[SwitchA] multicast-vlan 10
```

# Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchA-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchA-mvlan-10] quit
```

# Assign GigabitEthernet 1/0/4 to VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port multicast-vlan 10
[SwitchA-GigabitEthernet1/0/4] quit
```

4) Verify the configuration

# View the multicast VLAN information on Switch A.

```
[SwitchA] display multicast-vlan
```

```
 Total 1 multicast-vlan(s)

 Multicast vlan 10
   subvlan list:
    no subvlan
   port list:
    GE1/0/2                 GE1/0/3                 GE1/0/4
```

# View the IGMP Snooping multicast group information on Switch A.

```
[SwitchA] display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):10.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1                 (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 3 port.
            GE1/0/2                 (D)
            GE1/0/3                 (D)
            GE1/0/4                 (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 3 port.
            GE1/0/2
            GE1/0/3
            GE1/0/4
```

As shown above, IGMP Snooping is maintaining the router ports and member ports in VLAN 10.

# Table of Contents

# 1 MLD Snooping Configuration

When configuring MLD Snooping, go to these sections for information you are interested in:



## MLD Snooping Overview

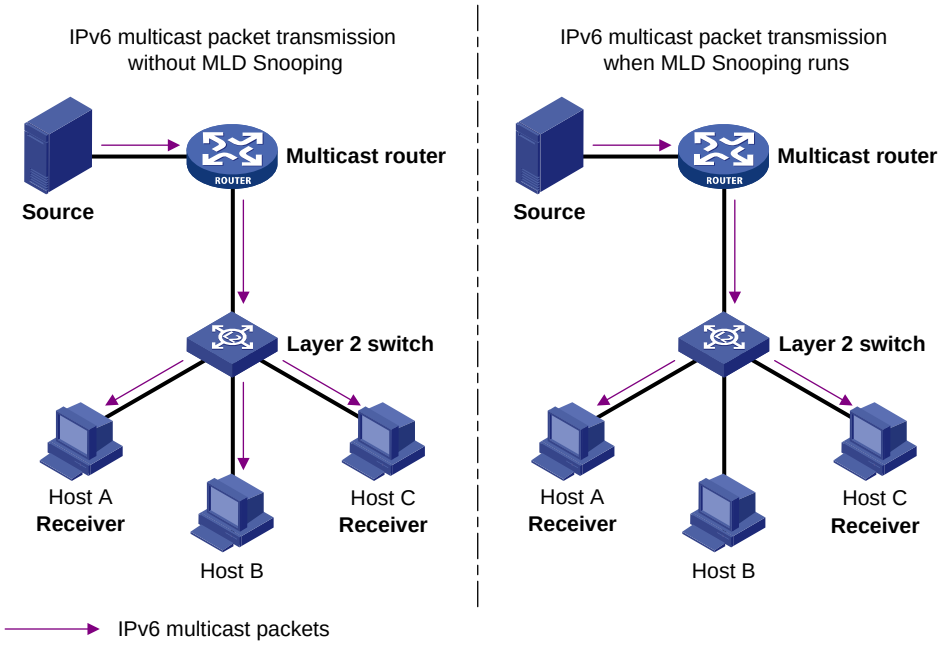
Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups.

### Introduction to MLD Snooping

By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

As shown in Figure 1-1, when MLD Snooping is not running, IPv6 multicast packets are broadcast to all devices at Layer 2. When MLD Snooping runs, multicast packets for known IPv6 multicast groups are multicast to the receivers at Layer 2.

**Figure 1-1** Before and after MLD Snooping is enabled on the Layer 2 device




MLD Snooping forwards multicast data to only the receivers requiring it at Layer 2. It brings the following advantages:

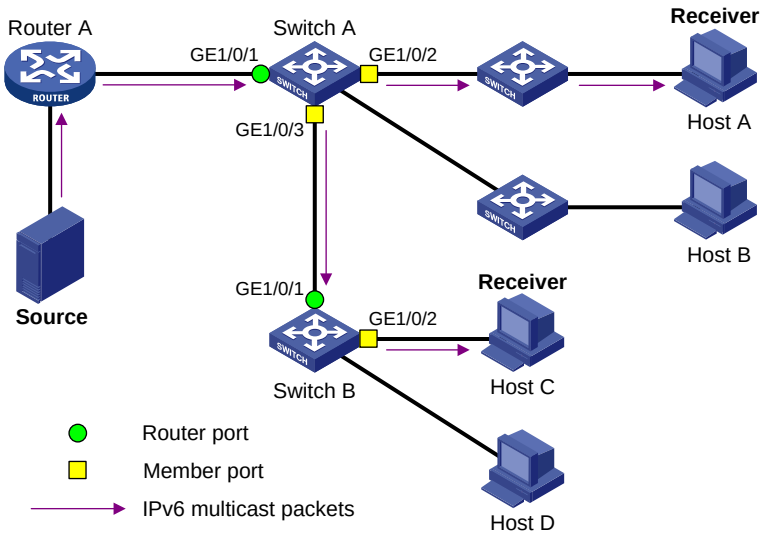
- Reducing Layer 2 broadcast packets, thus saving network bandwidth.
- Enhancing the security of multicast traffic.
- Facilitating the implementation of per-host accounting.

## Basic Concepts in MLD Snooping

### MLD Snooping related ports

As shown in Figure 1-2, Router A connects to the multicast source, MLD Snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, IPv6 multicast group members).

**Figure 1-2** MLD Snooping related ports




Ports involved in MLD Snooping, as shown in Figure 1-2, are described as follows:

- Router port: A router port is a port on the Ethernet switch that leads switch towards the Layer-3 multicast device (DR or MLD querier). In the figure, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. The switch registers all its local router ports in its router port list.
- Member port: A member port (also known as IPv6 multicast group member port) is a port on the Ethernet switch that leads towards multicast group members. In the figure, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. The switch registers all the member ports on the local device in its MLD Snooping forwarding table.

**Note**

- Whenever mentioned in this document, a router port is a router-connecting port on the switch, rather than a port on a router.
- Unless otherwise specified, router/member ports mentioned in this document include static and dynamic ports.
- On an MLD Snooping-enabled switch, the ports that received MLD general queries with the source address other than 0::0 or IPv6 PIM hello messages are dynamic router ports.

### Aging timers for dynamic ports in MLD Snooping

**Table 1-1** Aging timers for dynamic ports in MLD Snooping and related messages and actions

| Timer | Description | Message before expiry | Action after expiry |
|---|---|---|---|
| Dynamic router port aging timer | For each dynamic router port, the switch sets a timer initialized to the dynamic router port aging time. | MLD general query of which the source address is not 0::0 or IPv6 PIM hello. | The switch removes this port from its router port list. |
| Dynamic member port aging timer | When a port dynamically joins an IPv6 multicast group, the switch sets a timer for the port, which is initialized to the dynamic member port aging time. | MLD report message. | The switch removes this port from the MLD Snooping forwarding table. |

**Note**

The port aging mechanism of MLD Snooping works only for dynamic ports; a static port will never age out.

## How MLD Snooping Works

A switch running MLD Snooping performs different actions when it receives different MLD messages, as follows:

**Caution**

The description about adding or deleting a port in this section is only for a dynamic port. Static ports can be added or deleted only through the corresponding configurations. For details, see Configuring Static Ports.

### General queries

The MLD querier periodically sends MLD general queries to all hosts and routers (FF02::1) on the local subnet to find out whether IPv6 multicast group members exist on the subnet.

Upon receiving an MLD general query, the switch forwards it through all ports in the VLAN except the port on which it received the MLD query and performs the following:

- If the port on which it the switch received the MLD query is a dynamic router port in its router port list, the switch resets the aging timer for this dynamic router port.
- If the port is not included in its router port list, the switch adds it into its router port list as a dynamic router port and sets an aging timer for it.

### Membership reports

A host sends an MLD report to the MLD querier in the following circumstances:

- Upon receiving an MLD query, an IPv6 multicast group member host responds with an MLD report.
- When intended to join an IPv6 multicast group, a host sends an MLD report to the MLD querier to announce that it is interested in the multicast information addressed to that IPv6 multicast group.

Upon receiving an MLD report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported IPv6 multicast group, and performs the following to the receiving port:

- If no forwarding table entry exists for the reported IPv6 multicast group, the switch creates an entry, adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported IPv6 multicast group, but the port is not included in the outgoing port list for that group, the switch adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported IPv6 multicast group and the port is included in the outgoing port list, which means that this port is already a dynamic member port, the switch resets the member port aging timer for that port.

---

**Note**

A switch does not forward an MLD report through a non-router port. The reason is as follows: Due to the MLD report suppression mechanism applied on hosts, if the switch forwards a report message through a member port, all the attached hosts listening to the reported IPv6 multicast address will suppress their own reports upon receiving this report, and this will prevent the switch from knowing whether the reported multicast group still has active members attached to that port.

---

### Done messages

When a host leaves an IPv6 multicast group, the host sends an MLD done message to the multicast router.

When the switch receives an MLD done message on a dynamic member port, the switch first checks whether a forwarding table entry for the IPv6 multicast group address in the message exists, and, if one exists, whether the outgoing port list contains the port.

- If the forwarding table entry does not exist or if the outgoing port list does not contain the port, the switch discards the MLD done message instead of forwarding it to any port.
- If the forwarding table entry exists and the outgoing port list contains the port, the switch forwards the MLD done message to all router ports in the native VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that IPv6 multicast group address, the switch does not immediately remove the port from the outgoing port list of the forwarding table entry for that group; instead, it resets the aging timer for the port.

Upon receiving an MLD done message from a host, the MLD querier resolves the IPv6 multicast group address in the message and sends an MLD multicast-address-specific query to that IPv6 multicast group address through the port that received the MLD done message. Upon receiving the MLD multicast-address-specific query, the switch forwards it through all the router ports in the VLAN and all member ports for that IPv6 multicast group, and performs the following to the receiving port:

- If any MLD report in response to the MLD multicast-address-specific query is received on the port (suppose it is a dynamic member port) before its aging timer expires, this means that some host attached to the port is receiving or expecting to receive IPv6 multicast data for that IPv6 multicast group. The switch resets the aging timer for the port.
- If no MLD report in response to the MLD multicast-address-specific query is received on the port before its aging timer expires, this means that no hosts attached to the port are still listening to that IPv6 multicast group address. The switch removes the port from the outgoing port list of the forwarding table entry for that IPv6 multicast group when the aging timer expires.

### Protocols and Standards

MLD Snooping is documented in:

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

## MLD Snooping Configuration Task List

Complete these tasks to configure MLD Snooping:

| Task | | Remarks |
|---|---|---|
| Configuring Basic Functions of MLD Snooping | Enabling MLD Snooping | Required |
| | Configuring the Version of MLD Snooping | Optional |
| Configuring MLD Snooping Port Functions | Configuring Aging Timers for Dynamic Ports | Optional |
| | Configuring Static Ports | Optional |
| | Configuring Simulated Joining | Optional |
| | Configuring Fast Leave Processing | Optional |
| Configuring MLD Snooping Querier | Enabling MLD Snooping Querier | Optional |
| | Configuring MLD Queries and Responses | Optional |
| | Configuring Source IPv6 Addresses of MLD Queries | Optional |

| Task | | Remarks |
|---|---|---|
| Configuring an MLD Snooping Policy | Configuring an IPv6 Multicast Group Filter | Optional |
| | Configuring IPv6 Multicast Source Port Filtering | Optional |
| | Configuring MLD Report Suppression | Optional |
| | Configuring Maximum Multicast Groups that Can Be Joined on a Port | Optional |
| | Configuring IPv6 Multicast Group Replacement | Optional |

**Note**

- Configurations made in MLD Snooping view are effective for all VLANs, while configurations made in VLAN view are effective only for ports belonging to the current VLAN. For a given VLAN, a configuration made in MLD Snooping view is effective only if the same configuration is not made in VLAN view.
- Configurations made in MLD Snooping view are effective for all ports; configurations made in Ethernet port view are effective only for the current port; configurations made in Layer 2 aggregate port view are effect only for the current port; configurations made in port group view are effective only for all the ports in the current port group. For a given port, a configuration made in MLD Snooping view is effective only if the same configuration is not made in Ethernet port view, Layer 2 aggregate port view or port group view.
- For MLD Snooping, configurations made on a Layer 2 aggregate port do not interfere with configurations made on its member ports, nor do they take part in aggregation calculations; configurations made on a member port of the aggregate group will not take effect until it leaves the aggregate group.

# Configuring Basic Functions of MLD Snooping

## Configuration Prerequisites

Before configuring the basic functions of MLD Snooping, complete the following tasks:

- Configure the corresponding VLANs

Before configuring the basic functions of MLD Snooping, prepare the following data:

- The version of MLD Snooping

## Enabling MLD Snooping

Follow these steps to enable MLD Snooping:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable MLD Snooping globally and enter MLD Snooping view | **mld-snooping** | Required<br>Disabled by default |
| Return to system view | **quit** | — |

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable MLD Snooping in the VLAN | **mld-snooping enable** | Required<br>Disabled by default |

**Note**

- MLD Snooping must be enabled globally before it can be enabled in a VLAN.
- When you enable MLD Snooping in a specified VLAN, this function takes effect for ports in this VLAN only.

### Configuring the Version of MLD Snooping

By configuring the MLD Snooping version, you actually configure the version of MLD messages that MLD Snooping can process.

- MLD Snooping version 1 can process MLDv1 messages, but cannot analyze and process MLDv2 messages, which will be flooded in the VLAN.
- MLD Snooping version 2 can process MLDv1 and MLDv2 messages.

Follow these steps to configure the version of MLD Snooping:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure the version of MLD Snooping | **mld-snooping version** *version-number* | Optional<br>Version 1 by default |

**Caution**

If you switch MLD Snooping from version 2 to version 1, the system will clear all MLD Snooping forwarding entries from dynamic joining, and will:

- Keep forwarding entries from version 2 static (*, G) joining;
- Clear forwarding entries from version 2 static (S, G) joining, which will be restored when MLD Snooping is switched back to version 2.

For details about static joining, refer to Configuring Static Ports.

## Configuring MLD Snooping Port Functions

### Configuration Prerequisites

Before configuring MLD Snooping port functions, complete the following tasks:

- Enable MLD Snooping in the VLAN or enable MLD on the desired VLAN interface

- Configure the corresponding port groups

Before configuring MLD Snooping port functions, prepare the following data:

- Aging time of dynamic router ports,
- Aging timer of dynamic member ports, and
- IPv6 multicast group and IPv6 multicast source addresses

## Configuring Aging Timers for Dynamic Ports

If the switch receives no MLD general queries or IPv6 PIM hello messages on a dynamic router port, the switch removes the port from the router port list when the aging timer of the port expires.

If the switch receives no MLD reports for an IPv6 multicast group on a dynamic member port, the switch removes the port from the outgoing port list of the forwarding table entry for that IPv6 multicast group when the port aging timer expires.

If IPv6 multicast group memberships change frequently, you can set a relatively small value for the dynamic member port aging timer.

### Configuring aging timers for dynamic ports globally

Follow these steps to configure aging timers for dynamic ports globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Configure dynamic router port aging time | **router-aging-time** *interval* | Optional<br>260 seconds by default |
| Configure dynamic member port aging time | **host-aging-time** *interval* | Optional<br>260 seconds by default |

### Configuring aging timers for dynamic ports in a VLAN

Follow these steps to configure aging timers for dynamic ports in a VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure dynamic router port aging time | **mld-snooping**<br>**router-aging-time** *interval* | Optional<br>260 seconds by default |
| Configure dynamic member port aging time | **mld-snooping**<br>**host-aging-time** *interval* | Optional<br>260 seconds by default |

## Configuring Static Ports

If all the hosts attached to a port is interested in the IPv6 multicast data addressed to a particular IPv6 multicast group, you can configure that port as a static member port for that IPv6 multicast group.

You can configure a port of a switch to be a static router port, through which the switch can forward all IPv6 multicast data it received.

Follow these steps to configure static ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure the port(s) as static member port(s) | **mld-snooping static-group** *ipv6-group-address* [ **source-ip** *ipv6-source-address* ] **vlan** *vlan-id* | Required<br>No static member ports by default |
| Configure the port(s) as static router port(s) | **mld-snooping static-router-port** vlan *vlan-id* | Required<br>No static router ports by default |

**Note**

- An IPv6 static (S, G) join takes effect only if a valid IPv6 multicast source address is specified and MLD Snooping version 2 is currently running.
- A static member port does not respond to queries from the MLD querier; when static (*, G) or (S, G) joining is enabled or disabled on a port, the port does not send an unsolicited MLD report or an MLD done message.
- Static member ports and static router ports never age out. To remove such a port, you need to use the corresponding **undo** command.

## Configuring Simulated Joining

Generally, a host running MLD responds to MLD queries from the MLD querier. If a host fails to respond due to some reasons, the multicast router will deem that no member of this IPv6 multicast group exists on the network segment, and therefore will remove the corresponding forwarding path.

To avoid this situation from happening, you can enable simulated joining on a port of the switch, namely configure the port as a simulated member host for an IPv6 multicast group. When an MLD query is received, simulated host gives a response. Thus, the switch can continue receiving IPv6 multicast data.

A simulated host acts like a real host, as follows:

- When a port is configured as a simulated member host, the switch sends an unsolicited MLD report through that port.
- After a port is configured as a simulated member host, the switch responds to MLD general queries by sending MLD reports through that port.
- When the simulated joining function is disabled on a port, the switch sends an MLD done message through that port.

Follow these steps to configure simulated joining:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure simulated joining | **mld-snooping host-join** *ipv6-group-address* [ **source-ip** *ipv6-source-address* ] **vlan** *vlan-id* | Required<br>Disabled by default |

**Note**

- Each simulated host is equivalent to an independent host. For example, when receiving an MLD query, the simulated host corresponding to each configuration responds respectively.
- Unlike a static member port, a port configured as a simulated member host will age out like a dynamic member port.

## Configuring Fast Leave Processing

The fast leave processing feature allows the switch to process MLD done messages in a fast way. With the fast leave processing feature enabled, when receiving an MLD done message on a port, the switch immediately removes that port from the outgoing port list of the forwarding table entry for the indicated IPv6 multicast group. Then, when receiving MLD done multicast-address-specific queries for that IPv6 multicast group, the switch will not forward them to that port.

In VLANs where only one host is attached to each port, fast leave processing helps improve bandwidth and resource usage.

### Configuring fast leave processing globally

Follow these steps to configure fast leave processing globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Enable fast leave processing | **fast-leave** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

### Configuring fast leave processing on a port or a group of ports

Follow these steps to configure fast leave processing on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable fast leave processing | **mld-snooping fast-leave** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

**Caution**

If fast leave processing is enabled on a port to which more than one host is connected, when one host leaves an IPv6 multicast group, the other hosts connected to port and interested in the same IPv6 multicast group will fail to receive IPv6 multicast data addressed to that group.

# Configuring MLD Snooping Querier

## Configuration Prerequisites

Before configuring MLD Snooping querier, complete the following task:

- Enable MLD Snooping in the VLAN.

Before configuring MLD Snooping querier, prepare the following data:

- MLD general query interval,
- MLD last-member query interval,
- Maximum response time for MLD general queries,
- Source IPv6 address of MLD general queries, and
- Source IPv6 address of MLD multicast-address-specific queries.

## Enabling MLD Snooping Querier

In an IPv6 multicast network running MLD, a multicast router or Layer 3 multicast switch is responsible for sending periodic MLD general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called MLD querier.

However, a Layer 2 multicast switch does not support MLD, and therefore cannot send MLD general queries by default. By enabling MLD Snooping querier on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no Layer 3 multicast devices are present, the Layer 2 switch will act as the MLD querier to send periodic MLD queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Follow these steps to enable the MLD Snooping querier:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable the MLD Snooping querier | **mld-snooping querier** | Required<br>Disabled by default |

**Caution**

It is meaningless to configure an MLD Snooping querier in an IPv6 multicast network running MLD. Although an MLD Snooping querier does not take part in MLD querier elections, it may affect MLD querier elections because it sends MLD general queries with a low source IPv6 address.

## Configuring MLD Queries and Responses

You can tune the MLD general query interval based on actual condition of the network.

Upon receiving an MLD query (general query or multicast-address-specific query), a host starts a timer for each IPv6 multicast group it has joined. This timer is initialized to a random value in the range of 0 to the maximum response time (the host obtains the value of the maximum response time from the Max Response Time field in the MLD query it received). When the timer value comes down to 0, the host sends an MLD report to the corresponding IPv6 multicast group.

An appropriate setting of the maximum response time for MLD queries allows hosts to respond to queries quickly and avoids bursts of MLD traffic on the network caused by reports simultaneously sent by a large number of hosts when the corresponding timers expire simultaneously.

- For MLD general queries, you can configure the maximum response time to fill their Max Response time field.
- For MLD multicast-address-specific queries, you can configure the MLD last-member query interval to fill their Max Response time field. Namely, for MLD multicast-address-specific queries, the maximum response time equals to the MLD last-member query interval.

### Configuring MLD queries and responses globally

Follow these steps to configure MLD queries and responses globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Configure the maximum response time for MLD general queries | **max-response-time** *interval* | Optional<br>10 seconds by default |
| Configure the MLD last-member query interval | **last-listener-query-interval** *interval* | Optional<br>1 second by default |

### Configuring MLD queries and responses in a VLAN

Follow these steps to configure MLD queries and responses in a VLAN

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure MLD query interval | **mld-snooping query-interval** *interval* | Optional<br>125 seconds by default |
| Configure the maximum response time for MLD general queries | **mld-snooping max-response-time** *interval* | Optional<br>10 seconds by default |
| Configure the MLD last-member query interval | **mld-snooping last-listener-query-interval** *interval* | Optional<br>1 second by default |

**Caution**

Make sure that the MLD query interval is greater than the maximum response time for MLD general queries; otherwise undesired deletion of IPv6 multicast members may occur.

## Configuring Source IPv6 Addresses of MLD Queries

This configuration allows you to change the source IPv6 address of MLD queries.

Follow these steps to configure source IPv6 addresses of MLD queries:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure the source IPv6 address of MLD general queries | **mld-snooping general-query source-ip** { **current-interface** \| *ipv6-address* } | Optional<br>FE80::02FF:FFFF:FE00:0001 by default |
| Configure the source IPv6 address of MLD multicast-address-specific queries | **mld-snooping special-query source-ip** { **current-interface** \| *ipv6-address* } | Optional<br>FE80::02FF:FFFF:FE00:0001 by default |

**Caution**

The source IPv6 address of MLD query messages may affect MLD querier election within the segment.

# Configuring an MLD Snooping Policy

## Configuration Prerequisites

Before configuring an MLD Snooping policy, complete the following tasks:

- Enable MLD Snooping in the VLAN or enable MLD on the desired VLAN interface

Before configuring an MLD Snooping policy, prepare the following data:

- IPv6 ACL rule for IPv6 multicast group filtering
- The maximum number of IPv6 multicast groups that can pass the ports

## Configuring an IPv6 Multicast Group Filter

On a MLD Snooping–enabled switch, the configuration of an IPv6 multicast group filter allows the service provider to define limits of multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an MLD report. Upon receiving this report message, the switch checks the report against the configured ACL rule. If the port on which the report was received can join this IPv6 multicast group, the switch adds an entry for this port in the MLD Snooping forwarding table; otherwise the switch drops this report message. Any IPv6 multicast data that fails the ACL check will not be sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

### Configuring an IPv6 multicast group filter globally

Follow these steps to configure an IPv6 multicast group globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Configure an IPv6 multicast group filter | **group-policy** *acl6-number* [ **vlan** *vlan-list* ] | Required<br>No IPv6 filter configured by default. |

### Configuring an IPv6 multicast group filter on a port or a group of ports

Follow these steps to configure an IPv6 multicast group filer on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Configure an IPv6 multicast group filter | **mld-snooping group-policy** *acl6-number* [ **vlan** *vlan-list* ] | Required<br>No IPv6 filter configured by default. |

## Configuring IPv6 Multicast Source Port Filtering

With the IPv6 multicast source port filtering feature enabled on a port, the port can be connected with IPv6 multicast receivers only rather than with multicast sources, because the port will block all IPv6 multicast data packets while it permits multicast protocol packets to pass.

If this feature is disabled on a port, the port can be connected with both multicast sources and IPv6 multicast receivers.

### Configuring IPv6 multicast source port filtering globally

Follow these steps to configure IPv6 multicast source port filtering:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Enable IPv6 multicast source port filtering | **source-deny port** *interface-list* | Required<br>Disabled by default |

### Configuring IPv6 multicast source port filtering on a port or a group of ports

Follow these steps to configure IPv6 multicast source port filtering on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable IPv6 multicast source port filtering | **mld-snooping source-deny** | Required<br>Disabled by default |

**Note**

Some models of devices, when enabled to filter IPv6 multicast data based on the source ports, are automatically enabled to filter IPv4 multicast data based on the source ports.

## Configuring MLD Report Suppression

When a Layer 2 device receives an MLD report from an IPv6 multicast group member, the Layer 2 device forwards the message to the Layer 3 device directly connected with it. Thus, when multiple members belonging to an IPv6 multicast group exist on the Layer 2 device, the Layer 3 device directly connected with it will receive duplicate MLD reports from these members.

With the MLD report suppression function enabled, within a query interval, the Layer 2 device forwards only the first MLD report of an IPv6 group to the Layer 3 device and will not forward the subsequent

MLD reports from the same multicast group to the Layer 3 device. This helps reduce the number of packets being transmitted over the network.

Follow these steps to configure MLD report suppression:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Enable MLD report suppression | **report-aggregation** | Optional<br>Enabled by default |

## Configuring Maximum Multicast Groups that Can Be Joined on a Port

By configuring the maximum number of IPv6 multicast groups that can be joined on a port or a group of ports, you can limit the number of multicast programs available to VOD users, thus to control the traffic on the port.

Follow these steps configure the maximum number of IPv6 multicast groups that can be joined on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number*<br>**port-group manual** *port-group-name* | Required<br>Use either approach |
| Configure the maximum number of IPv6 multicast groups that can be joined on a port | **mld-snooping group-limit** *limit* [ **vlan** *vlan-list* ] | Optional<br>128 by default. |

Note

- When the number of IPv6 multicast groups that can be joined on a port reaches the maximum number configured, the system deletes all the forwarding entries persistent to that port from the MLD Snooping forwarding table, and the hosts on this port need to join IPv6 multicast groups again.
- If you have configured static or simulated joining on a port, however, when the number of IPv6 multicast groups on the port exceeds the configured threshold, the system deletes all the forwarding entries persistent to that port from the MLD Snooping forwarding table and applies the static or simulated joining again, until the number of IPv6 multicast groups joined by the port comes back within the configured threshold.

## Configuring IPv6 Multicast Group Replacement

For some special reasons, the number of IPv6 multicast groups passing through a switch or port may exceed the number configured for the switch or the port. In addition, in some specific applications, an IPv6 multicast group newly joined on the switch needs to replace an existing IPv6 multicast group automatically. A typical example is “channel switching”, namely, by joining the new multicast group, a user automatically switches from the current IPv6 multicast group to the new one.

To address this situation, you can enable the IPv6 multicast group replacement function on the switch or certain ports. When the number of IPv6 multicast groups a switch or a port has joined exceeds the limit.

- If the IPv6 multicast group replacement is enabled, the newly joined IPv6 multicast group automatically replaces an existing IPv6 multicast group with the lowest IPv6 address.
- If the IPv6 multicast group replacement is not enabled, new MLD reports will be automatically discarded.

### Configuring IPv6 multicast group replacement globally

Follow these steps to configure IPv6 multicast group replacement globally:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter MLD Snooping view | **mld-snooping** | — |
| Enable IPv6 multicast group replacement | **overflow-replace** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

### Configuring IPv6 multicast group replacement on a port or a group of ports

Follow these steps to configure IPv6 multicast group replacement on a port or a group of ports:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port/Layer 2 aggregate port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach |
| | **port-group manual** *port-group-name* | |
| Enable IPv6 multicast group replacement | **mld-snooping overflow-replace** [ **vlan** *vlan-list* ] | Required<br>Disabled by default |

**Caution**

Be sure to configure the maximum number of IPv6 multicast groups allowed on a port (refer to Configuring Maximum Multicast Groups that Can Be Joined on a Port) before enabling IPv6 multicast group replacement. Otherwise, the IPv6 multicast group replacement functionality will not take effect.

## Displaying and Maintaining MLD Snooping

| To do… | Use the command... | Remarks |
|---|---|---|
| View MLD Snooping multicast group information | **display mld-snooping group** [ **vlan** *vlan-id* ] [ **verbose** ] | Available in any view |
| View the statistics information of MLD messages learned by MLD Snooping | **display mld-snooping statistics** | Available in any view |
| Clear MLD Snooping multicast group information | **reset mld-snooping group** { *ipv6-group-address* \| **all** } [ **vlan** *vlan-id* ] | Available in user view |
| Clear the statistics information of all kinds of MLD messages learned by MLD Snooping | **reset mld-snooping statistics** | Available in user view |

**Note**

- The **reset mld-snooping group** command works on an MLD Snooping–enabled VLAN.
- The **reset mld-snooping group** command cannot clear the MLD Snooping multicast group information for static joining.

# MLD Snooping Configuration Examples

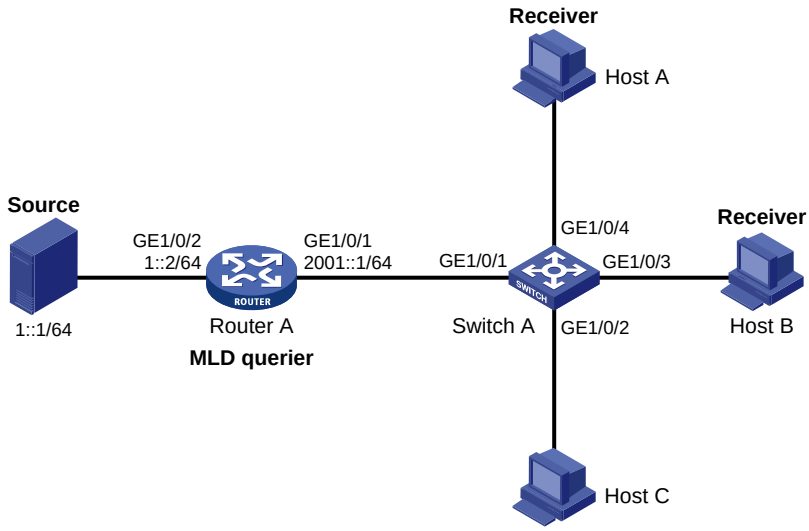
## Configuring IPv6 Group Policy and Simulated Joining

### Network requirements

- As shown in Figure 1-3, Router A connects to the IPv6 multicast source through GigabitEthernet 1/0/2 and to Switch A through GigabitEthernet 1/0/1. Router A is the MLD querier on the subnet.
- MLDv1 is required on Router A, MLD Snooping version 1 is required on Switch A, and Router A will act as the MLD querier on the subnet.
- It is required that the receivers, Host A and Host B, attached to Switch A can receive IPv6 multicast traffic addressed to IPv6 multicast group FF1E::101 only.
- It is required that IPv6 multicast data for group FF1E::101 can be forwarded through GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A even if Host A and Host B accidentally, temporarily stop receiving IPv6 multicast data.

### Network diagram

**Figure 1-3** Network diagram for IPv6 group policy simulated joining configuration




### Configuration procedure

1) Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as per Figure 1-3. The detailed configuration steps are omitted.

2) Configure Router A

# Enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLDv1 on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

# Enable MLD Snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable MLD Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

# Configure an IPv6 multicast group filter so that the hosts in VLAN 100 can join only the IPv6 multicast group FF1E::101.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA–mld-snooping] group-policy 2001 vlan 100
[SwitchA–mld-snooping] quit
```

# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated hosts for IPv6 multicast group FF1E::101.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

4) Verify the configuration

# View the detailed MLD Snooping multicast group information in VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/1               (D) ( 00:01:30 )
    IP group(s):the following ip group(s) match to one mac group.
```

```
  IP group address:FF1E::101
    (::, FF1E::101):
      Attribute:    Host Port
      Host port(s):total 2 port.
        GE1/0/3                (D) ( 00:03:23 )
        GE1/0/4                (D) ( 00:04:10 )
MAC group(s):
  MAC group address:3333-0000-1001
      Host port(s):total 2 port.
        GE1/0/3
        GE1/0/4
```

As shown above, GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A have joined IPv6 multicast group FF1E::101.

## Static Port Configuration

### Network requirements

- As shown in Figure 1-4, Router A connects to an IPv6 multicast source (Source) through GigabitEthernet 1/0/2, and to Switch A through GigabitEthernet 1/0/1.
- MLDv1 is to run on Router A, and MLDv1 Snooping is to run on Switch A, Switch B and Switch C, with Router A acting as the MLD querier.
- Host A and host C are permanent receivers of IPv6 multicast group FF1E::101. GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C are required to be configured as static member ports for multicast group 224.1.1.1 to enhance the reliability of multicast traffic transmission.
- Suppose STP runs on the network. To avoid data loops, the forwarding path from Switch A to Switch C is blocked under normal conditions, and IPv6 multicast traffic flows to the receivers attached to Switch C only along the path of Switch A—Switch B—Switch C.
- It is required to configure GigabitEthernet 1/0/3 that connects Switch A to Switch C as a static router port, so that IPv6 multicast traffic can flow to the receivers nearly uninterruptedly along the path of Switch A—Switch C in the case that the path of Switch A—Switch B—Switch C gets blocked.

---

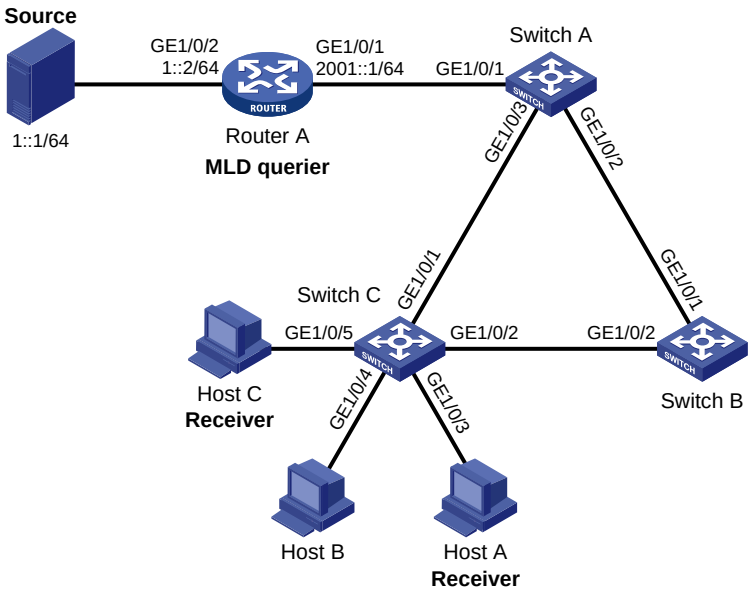
**Note**

If no static router port is configured, when the path of Switch A—Switch B—Switch C gets blocked, at least one MLD query-response cycle must be completed before the IPv6 multicast data can flow to the receivers along the new path of Switch A—Switch C, namely IPv6 multicast delivery will be interrupted during this process.

---

## Network diagram

**Figure 1-4** Network diagram for static port configuration




## Configuration procedure

1) Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as per Figure 1-4.

2) Configure Router A

# Enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLD on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

# Enable MLD Snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable MLD Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchA-vlan100] mld-snooping enable
```

```
[SwitchA-vlan100] quit
```

# Configure GigabitEthernet 1/0/3 to be a static router port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4) Configure Switch B

# Enable MLD Snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to this VLAN, and enable MLD Snooping in the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

5) Configure Switch C

# Enable MLD Snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to this VLAN, and enable MLD Snooping in the VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for IPv6 multicast group FF1E::101.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface GigabitEthernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

6) Verify the configuration

# View the detailed MLD Snooping multicast group information in VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 2 port.
            GE1/0/1               (D) ( 00:01:30 )
            GE1/0/3               (S)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Attribute:    Host Port
          Host port(s):total 1 port.
            GE1/0/2               (D) ( 00:03:23 )
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/2
```

As shown above, GigabitEthernet 1/0/3 of Switch A has become a static router port.

# View the detailed MLD Snooping multicast group information in VLAN 100 on Switch C.

```
[SwitchC] display mld-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            GE1/0/2               (D) ( 00:01:23 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Attribute:    Host Port
          Host port(s):total 2 port.
            GE1/0/3               (S)
            GE1/0/5               (S)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 2 port.
            GE1/0/3
            GE1/0/5
```

As shown above, GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for IPv6 multicast group FF1E::101.

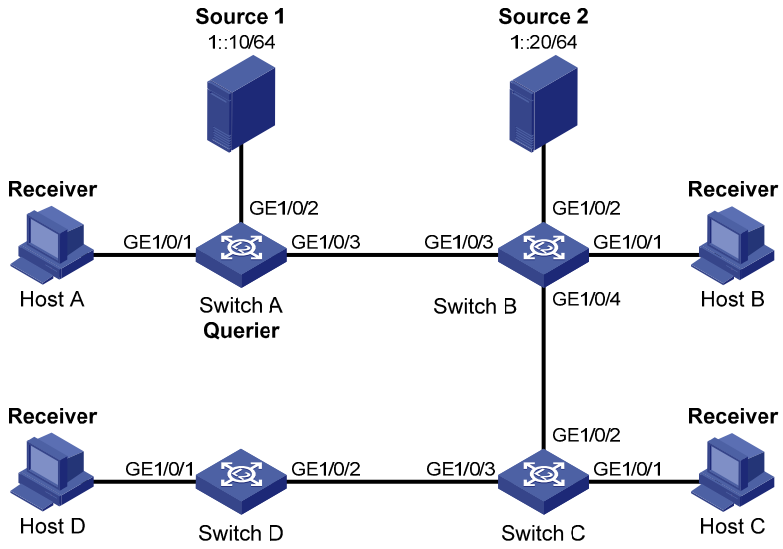
# MLD Snooping Querier Configuration

## Network requirements

- As shown in Figure 1-5, in a Layer-2-only network environment, two multicast sources Source 1 and Source 2 send IPv6 multicast data to multicast groups FF1E::101 and FF1E::102 respectively, Host A and Host C are receivers of multicast group FF1E::101, while Host B and Host D are receivers of multicast group FF1E::102.
- MLDv1 is enabled on all the receivers and MLDv1 Snooping is enabled on all the switches. Switch A, which is close to the multicast sources, is chosen as the MLD Snooping querier.

## Network diagram

**Figure 1-5** Network diagram for MLD Snooping querier configuration




## Configuration procedure

1) Configure Switch A

# Enable IPv6 forwarding and enable MLD Snooping globally.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

# Enable MLD Snooping and configure MLD Snooping querier feature in VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping querier
[SwitchA-vlan100] quit
```

2) Configure Switch B

# Enable IPv6 forwarding and enable MLD Snooping globally.

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# Create VLAN 100, add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 into VLAN 100.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable the MLD Snooping feature in VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

Configurations of Switch C and Switch D are similar to the configuration of Switch B.

3) Verify the configuration

When the MLD Snooping querier starts to work, all the switches but the querier receive MLD general queries. Use the **display mld-snooping statistics** command to view the statistics information of these MLD messages received.

# View the MLD message statistics on Switch B.

```
[SwitchB-vlan100] display mld-snooping statistics
  Received MLD general queries:3.
  Received MLDv1 specific queries:0.
  Received MLDv1 reports:12.
  Received MLD dones:0.
  Sent     MLDv1 specific queries:0.
  Received MLDv2 reports:0.
  Received MLDv2 reports with right and wrong records:0.
  Received MLDv2 specific queries:0.
  Received MLDv2 specific sg queries:0.
  Sent     MLDv2 specific queries:0.
  Sent     MLDv2 specific sg queries:0.
  Received error MLD messages:0.
```

# Troubleshooting MLD Snooping

## Switch Fails in Layer 2 Multicast Forwarding

### Symptom

A switch fails to implement Layer 2 multicast forwarding.

### Analysis

MLD Snooping is not enabled.

### Solution

1) Enter the **display current-configuration** command to view the running status of MLD Snooping.
2) If MLD Snooping is not enabled, use the **mld-snooping** command to enable MLD Snooping globally, and then use **mld-snooping enable** command to enable MLD Snooping in VLAN view.
3) If MLD Snooping is disabled only for the corresponding VLAN, just use the **mld-snooping enable** command in VLAN view to enable MLD Snooping in the corresponding VLAN.

## Configured IPv6 Multicast Group Policy Fails to Take Effect

### Symptom

Although an IPv6 multicast group policy has been configured to allow hosts to join specific IPv6 multicast groups, the hosts can still receive IPv6 multicast data addressed to other groups.

### Analysis

- The IPv6 ACL rule is incorrectly configured.
- The IPv6 multicast group policy is not correctly applied.

### Solution

1) Use the **display acl ipv6** command to check the configured IPv6 ACL rule. Make sure that the IPv6 ACL rule conforms to the IPv6 multicast group policy to be implemented.
2) Use the **display this** command in MLD Snooping view or the corresponding port view to check whether the correct IPv6 multicast group policy has been applied. If not, use the **group-policy** or **mld-snooping group-policy** command to apply the correct IPv6 multicast group policy.

# Table of Contents

# 1 IPv6 Multicast VLAN Configuration

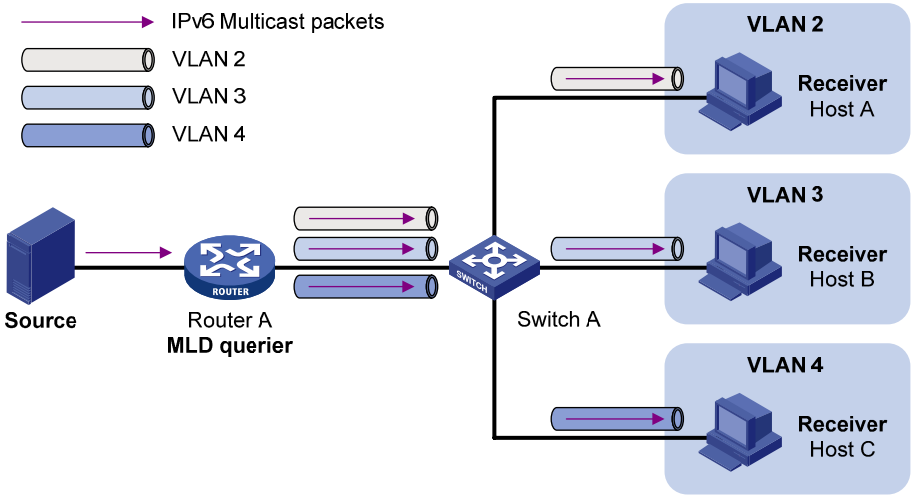
When configuring IPv6 multicast VLAN, go to these sections for information you are interested in:



## Introduction to IPv6 Multicast VLAN

As shown in Figure 1-1, in the traditional IPv6 multicast programs-on-demand mode, when hosts, Host A, Host B and Host C, belonging to different VLANs require IPv6 multicast programs on demand service, the Layer 3 device, Router A, needs to forward a separate copy of the multicast traffic in each user VLAN to the Layer 2 device, Switch A. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

**Figure 1-1** Multicast transmission without IPv6 multicast VLAN



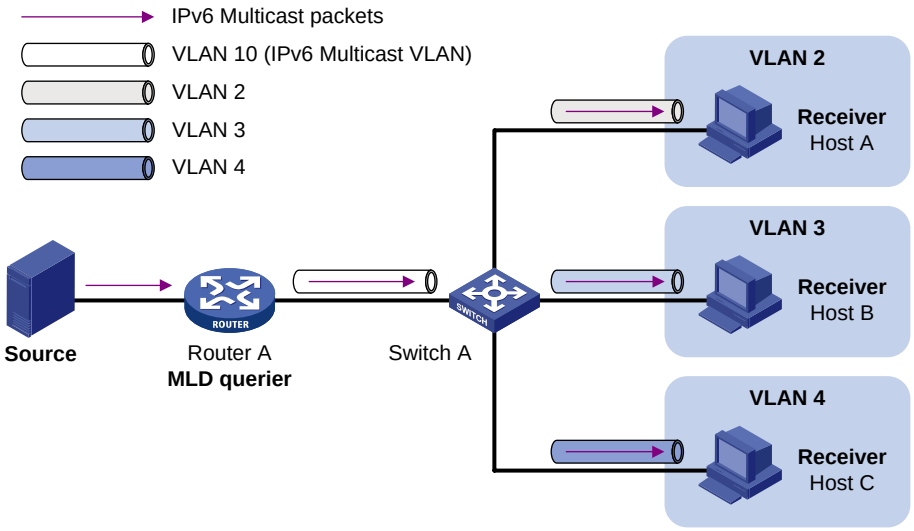

The IPv6 multicast VLAN feature configured on the Layer 2 device is the solution to this issue. With the IPv6 multicast VLAN feature, the Layer 3 device needs to replicate the multicast traffic only in the IPv6 multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This saves the network bandwidth and lessens the burden of the Layer 3 device.

The IPv6 multicast VLAN feature can be implemented in two approaches, as described below:

### Sub-VLAN-based IPv6 multicast VLAN

As shown in Figure 1-2, Host A, Host B and Host C are in three different user VLANs. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, configure all the user VLANs as sub-VLANs of this IPv6 multicast VLAN, and enable MLD snooping in the IPv6 multicast VLAN.

**Figure 1-2** Sub-VLAN-based IPv6 multicast VLAN

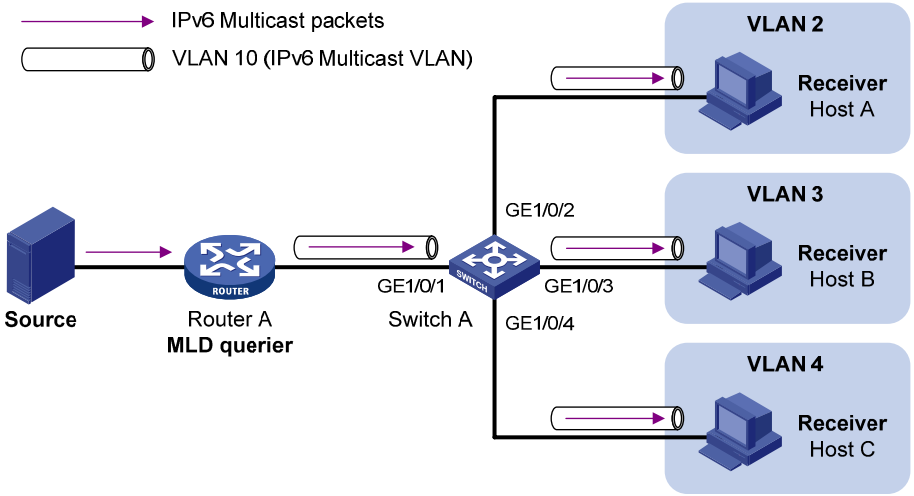



After the configuration, MLD snooping manages router ports in the IPv6 multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the IPv6 multicast VLAN, and Switch A distributes the traffic to the IPv6 multicast VLAN's sub-VLANs that contain receivers.

## Port-based IPv6 multicast VLAN

As shown in Figure 1-3, Host A, Host B and Host C are in three different user VLANs. All the user ports are hybrid ports. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, assign all the user ports to this IPv6 multicast VLAN, and enable MLD Snooping in the IPv6 multicast VLAN and all the user VLANs.

**Figure 1-3** Port-based IPv6 multicast VLAN




After the configuration, upon receiving an MLD message on a user port, Switch A tags the message with the IPv6 multicast VLAN ID and relays it to the MLD querier, so that MLD Snooping can uniformly manage the router ports and member ports in the IPv6 multicast VLAN. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the IPv6 multicast VLAN, and Switch A distributes the traffic to all the member ports in the IPv6 multicast VLAN.

**Note**

- For information about MLD Snooping, router ports, and member ports, refer to *MLD Snooping Configuration* in the *IP Multicast Volume*.
- For information about VLAN tags, refer to *VLAN Configuration* in the *Access Volume*.

# IPv6 Multicast VLAN Configuration Task List

Complete the following tasks to configure IPv6 multicast VLAN:

| Configuration task | | Remarks |
|---|---|---|
| Configuring IPv6 Sub-VLAN-Based IPv6 Multicast VLAN | | Required<br>Use either approach. |
| Configuring Port-Based IPv6 Multicast VLAN | Configuring User Port Attributes | |
| | Configuring IPv6 Multicast VLAN Ports | |

**Note**

If you have configured both sub-VLAN-based IPv6 multicast VLAN and port-based IPv6 multicast VLAN on a device, the port-based IPv6 multicast VLAN configuration is given preference.

# Configuring IPv6 Sub-VLAN-Based IPv6 Multicast VLAN

## Configuration Prerequisites

Before configuring sub-VLAN-based IPv6 multicast VLAN, complete the following tasks:

- Create VLANs as required
- Enable MLD Snooping in the VLAN to be configured as an IPv6 multicast VLAN

## Configuring Sub-VLAN-Based IPv6 Multicast VLAN

In this approach, you configure a VLAN as an IPv6 multicast VLAN, and configure user VLANs as sub-VLANs of the IPv6 multicast VLAN.

Follow these steps to configure sub-VLAN-based IPv6 multicast VLAN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view | **multicast-vlan ipv6** *vlan-id* | Required<br>No IPv6 multicast VLAN configured by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the specified VLAN(s) as sub-VLAN(s) of the IPv6 multicast VLAN | **subvlan** *vlan-list* | Required<br>By default, an IPv6 multicast VLAN has no sub-VLANs. |

**Note**

- The VLAN to be configured as an IPv6 multicast VLAN must exist.
- The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be sub-VLANs of another IPv6 multicast VLAN.
- The total number of sub-VLANs of an IPv6 multicast VLAN must not exceed 63.

# Configuring Port-Based IPv6 Multicast VLAN

When configuring port-based IPv6 multicast VLAN, you need to configure the attributes of each user port and then assign the ports to the IPv6 multicast VLAN.

**Note**

- A user port can be configured as a multicast VLAN port only if it is of the Ethernet or Layer 2 aggregate port type.
- Configurations made in Ethernet port view are effective only for the current port; configurations made in Layer 2 aggregate port view are effective only for the current port; configurations made in port group view are effective for all the ports in the current port group.

## Configuration Prerequisites

Before configuring port-based IPv6 multicast VLAN, complete the following tasks:

- Create VLANs as required
- Enable MLD Snooping in the VLAN to be configured as an IPv6 multicast VLAN
- Enable MLD Snooping in all the user VLANs

## Configuring User Port Attributes

Configure the user ports as hybrid ports to permit packets of the specified user VLAN to pass and configure the user VLAN to which the user ports belong as the default VLAN.

Configure the user ports to permit packets of the IPv6 multicast VLAN to pass and untag the packets. Thus, upon receiving multicast packets tagged with the IPv6 multicast VLAN ID from the upstream device, the Layer 2 device untags the multicast packets and forwards them to its downstream device.

Follow these steps to configure user port attributes:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either approach. |
| | **port-group manual** *port-group-name* | |
| Configue the user port link type as hybrid | **port link-type hybrid** | Required<br>Access by default |
| Specify the user VLAN that comprises the current user port(s) as the default VLAN | **port hybrid pvid vlan** *vlan-id* | Required<br>VLAN 1 by default |
| Configure the current user ports to permit packets of the specified IPv6 multicast VLAN to pass and untag the packets | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required<br>By default, a hybrid port permits only packets of VLAN 1 to pass. |

**Note**

For details about the **port link-type**, **port hybrid pvid vlan**, and **port hybrid vlan** commands, refer to VLAN Commands in the Access Volume.

## Configuring IPv6 Multicast VLAN Ports

In this approach, you need to configure a VLAN as an IPv6 multicast VLAN and then assign user ports to this IPv6 multicast VLAN by either adding the user ports in the IPv6 multicast VLAN or specifying the IPv6 multicast VLAN on the user ports. These two methods give the same result.

### Configure IPv6 multicast VLAN ports in IPv6 multicast VLAN view

Follow these steps to configure IPv6 multicast VLAN ports in IPv6 multicast VLAN view:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view | **multicast-vlan ipv6** *vlan-id* | Required<br>No IPv6 multicast VLAN configured by default |
| Assign port(s) to the IPv6 multicast VLAN | **port** *interface-list* | Required<br>By default, an IPv6 multicast VLAN has no ports. |

### Configure IPv6 multicast VLAN ports in terface view or port group view

Follow these steps to configure IPv6 multicast VLAN ports in port view or port group view:

| To do… | Use this command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view | **multicast-vlan ipv6** *vlan-id* | Required<br>Not an IPv6 multicast VLAN by default. |
| Return to system view | **quit** | — |
| Enter port view or port group view | **interface** *interface-type interface-number* | Required<br>Use either command. |
| | **port-group manual** *port-group-name* | |
| Configure the port(s) as port(s) of the IPv6 muticast VLAN | **port multicast-vlan ipv6** *vlan-id* | Required<br>By default, a user port does not belong to any IPv6 multicast VLAN. |

**Note**

- The VLAN to be configured as an IPv6 multicast VLAN must exist.
- A port can belong to only one IPv6 multicast VLAN.

## Displaying and Maintaining IPv6 Multicast VLAN

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about an IPv6 multicast VLAN | **display multicast-vlan ipv6** [ *vlan-id* ] | Available in any view |

## IPv6 Multicast VLAN Configuration Examples

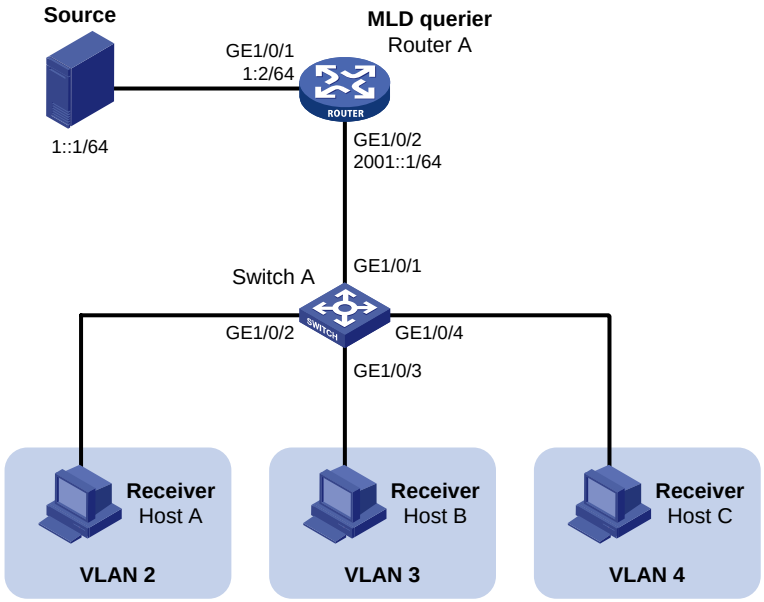
### Sub-VLAN-Based Multicast VLAN Configuration Example

#### Network requirements

- As shown in Figure 1-4, Router A connects to an IPv6 multicast source through GigabitEthernet 1/0/1 and to Switch A, through GigabitEthernet 1/0/2.
- MLDv1 is required on Router A, and MLD Snooping is required on Switch A. Router A is the MLD querier.
- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 of Switch A.
- The IPv6 multicast source sends IPv6 multicast data to the IPv6 multicast group FF1E::101. Host A, Host B, and Host C are receivers of the IPv6 multicast group.

- Configure the sub-VLAN-based IPv6 multicast VLAN feature so that Router A just sends IPv6 multicast data to Switch A through the IPv6 multicast VLAN and Switch A forwards the traffic to the receivers that belong to different user VLANs.

**Figure 1-4** Network diagram for sub-VLAN-based IPv6 multicast VLAN configuration




## Configuration procedure

1) Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding on each device and configure an IPv6 address and address prefix for each interface as per Figure 1-4. The detailed configuration steps are omitted here.

2) Configure Router A

# Enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface and enable MLD on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] mld enable
```

3) Configure Switch A

# Enable MLD Snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 2 and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar to the configuration for VLAN 2.

# Create VLAN 10, assign GigabitEthernet 1/0/1 to this VLAN and enable MLD Snooping in the VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

# Configure VLAN 10 as an IPv6 multicast VLAN and configure VLAN 2 through VLAN 4 as its sub-VLANs.

```
[SwitchA] multicast-vlan ipv6 10
[SwitchA-ipv6-mvlan-10] subvlan 2 to 4
[SwitchA-ipv6-mvlan-10] quit
```

4) Verify the configuration

# Display information about the IPv6 multicast VLAN.

```
[SwitchA] display multicast-vlan ipv6
 Total 1 IPv6 multicast-vlan(s)
 IPv6 Multicast vlan 10
   subvlan list:
    vlan 2-4
   port list:
    no port
```

# View the MLD Snooping IPv6 multicast group information on Switch A.

```
[SwitchA] display mld-snooping group
  Total 4 IP Group(s).
  Total 4 IP Source(s).
  Total 4 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:FF1E::101
        (::, FF1E::101):
          Host port(s):total 1 port.
            GE1/0/2                (D)
    MAC group(s):
      MAC group address:3333-0000-0101
          Host port(s):total 1 port.
            GE1/0/2
  Vlan(id):3.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
```

```
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 1 port.
          GE1/0/3                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 1 port.
          GE1/0/3
Vlan(id):4.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port.
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 1 port.
          GE1/0/4                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 1 port.
          GE1/0/4
Vlan(id):10.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
          GE1/0/1                (D)
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 0 port.
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 0 port.
```

As shown above, MLD Snooping is maintaining the router port in the IPv6 multicast VLAN (VLAN 10) and the member ports in the sub-VLANs (VLAN 2 through VLAN 4).

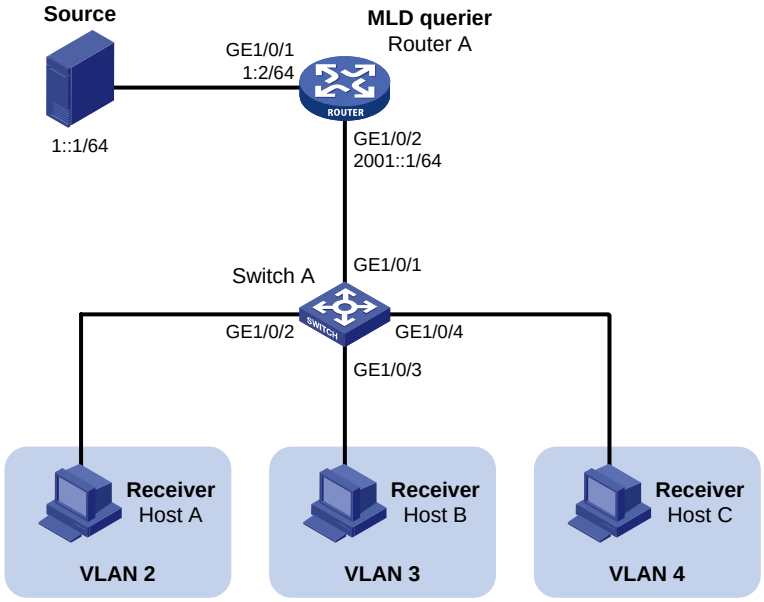
## Port-Based Multicast VLAN Configuration Example

### Network requirements

- As shown in Figure 1-5, Router A connects to an IPv6 multicast source (Source) through GigabitEthernet 1/0/1, and to Switch A through GigabitEthernet 1/0/2.
- MLDv1 is required on Router A. MLDv1 Snooping is required on Switch A. Router A acts as the MLD querier.

- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 of Switch A.
- The IPv6 multicast source sends IPv6 multicast data to IPv6 multicast group FF1E::101. Host A, Host B, and Host C are receivers of the IPv6 multicast group.
- Configure the port-based IPv6 multicast VLAN feature so that Router A just sends IPv6 multicast data to Switch A through the IPv6 multicast VLAN and Switch A forward the IPv6 multicast data to the receivers that belong to different user VLANs.

**Figure 1-5** Network diagram for port-based IPv6 multicast VLAN configuration




## Configuration procedure

1) Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding on each device and configure the IPv6 address and address prefix for each interface as per Figure 1-5. The detailed configuration steps are omitted here.

2) Configure Router A

# Enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLD on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] mld enable
```

3) Configure Switch A

# Enable MLD Snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 10, assign GigabitEthernet 1/0/1 to VLAN 10, and enable MLD Snooping in this VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

# Create VLAN 2 and enable MLD Snooping in the VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] mld-snooping enable
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar. The detailed configuration steps are omitted.

# Configure GigabitEthernet 1/0/2 as a hybrid port. Configure VLAN 2 as the default VLAN. Configue GigabitEthernet 1/0/2 to permit packets of VLAN 2 to pass and untag the packets when forwarding them.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

The configuration for GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 is similar. The detailed configuration steps are omitted.

# Configure VLAN 10 as an IPv6 multicast VLAN.

```
[SwitchA] multicast-vlan ipv6 10
```

# Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to IPv6 multicast VLAN 10.

```
[SwitchA-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchA-ipv6-mvlan-10] quit
```

# Assign GigabitEthernet 1/0/4 to IPv6 multicast VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port multicast-vlan ipv6 10
[SwitchA-GigabitEthernet1/0/4] quit
```

4) Verify the configuration

# View the IPv6 multicast VLAN information on Switch A.

```
[SwitchA] display multicast-vlan ipv6
 Total 1 IPv6 multicast-vlan(s)
 IPv6 Multicast vlan 10
   subvlan list:
    no subvlan
   port list:
    GE1/0/2                GE1/0/3                GE1/0/4
```

# View the MLD Snooping multicast group information on Switch A.

```
[SwitchA] display mld-snooping group
  Total 1 IP Group(s).
  Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):10.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
          GE1/0/1                (D)
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 3 port.
          GE1/0/2                (D)
          GE1/0/3                (D)
          GE1/0/4                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 3 port.
          GE1/0/2
          GE1/0/3
          GE1/0/4
```

As shown above, MLD Snooping is maintaining router ports and member ports in VLAN 10.

# QoS Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The QoS Volume is organized as follows:

| Features | Description |
|---|---|
| QoS | This document describes:<br>• QoS overview<br>• Traffic classification configuration<br>• Traffic policing Configuration<br>• Line rate configuration<br>• QoS policy configuration<br>• Congestion management<br>• Priority mapping configuration<br>• Traffic mirroring configuration |
| User Profile | User profile provides a configuration template to save predefined configurations. This document describes:<br>• Creating a User Profile<br>• Configuring a User Profile<br>• Enabling a User Profile |

# Table of Contents

# 1 QoS Overview

This chapter covers these topics:



## Introduction

Quality of Service (QoS) is a concept concerning service demand and supply. It reflects the ability to meet customer needs. Generally, QoS focuses on improving services under certain conditions rather than grading services precisely.

In an internet, QoS evaluates the ability of the network to forward packets using different services. The evaluation can be based on different criteria because the network may provide various services. Generally, QoS refers to the ability to provide improved service by solving the core issues such as delay, jitter, and packet loss ratio in the packet forwarding process.

## Traditional Packet Forwarding Service

On traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, reliability and so on.

This service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer and e-mail.

## New Requirements from Emerging Services

The Internet has been growing along with the fast development of networking technologies. More and more people use the Internet to transmit data, share video and do a lot of other things.

Besides traditional applications such as WWW, e-mail and FTP, network users are enjoying new services such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together with VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet.

These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For example, videoconference and VoD require high bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require high bandwidth but do require low delay and preferential service during congestion.

The emerging applications demand higher service performance of IP networks. Better network services during packets forwarding are required, such as providing dedicated bandwidth, reducing packet loss ratio, managing and avoiding congestion, regulating network traffic, and setting the precedence of packets. To meet these requirements, a network must provide more improved services.

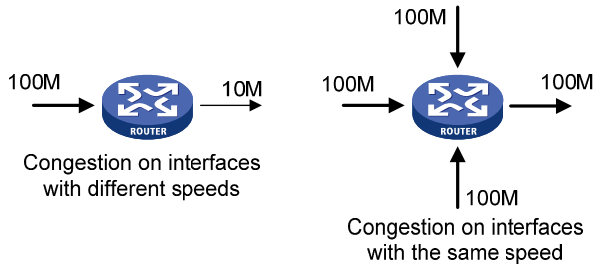
# Congestion: Causes, Impacts, and Countermeasures

Network congestion is a major factor degrading the service quality of a traditional network. Congestion is a situation where the forwarding rate decreases due to insufficient resources, resulting in extra delay.

## Causes

Congestion easily occurs in complex packet switching circumstances in the Internet. The following figure shows two common cases:

**Figure 1-1** Traffic congestion causes




- The traffic enters a device from a high speed link and is forwarded over a low speed link.
- The packet flows enter a device from several interfaces at the same rate and are forwarded out an interface at the same rate as well.

When traffic arrives at the line speed, a bottleneck will be created at the outgoing interface causing congestion.

Besides bandwidth bottlenecks, congestion can be caused by resource shortage in various forms such as insufficient processor time, buffer, and memory, and by network resource exhaustion resulting from excessive arriving traffic in certain periods.

## Impacts

Congestion may bring these negative results:

- Increased delay and jitter during packet transmission
- Decreased network throughput and resource use efficiency
- Network resource (memory in particular) exhaustion and even system breakdown

It is obvious that congestion hinders resource assignment for traffic and thus degrades service performance. The chance of congestion is high in switched networks and multi-user application environments. To improve the service performance of your network, you must address the congestion issues.

## Countermeasures

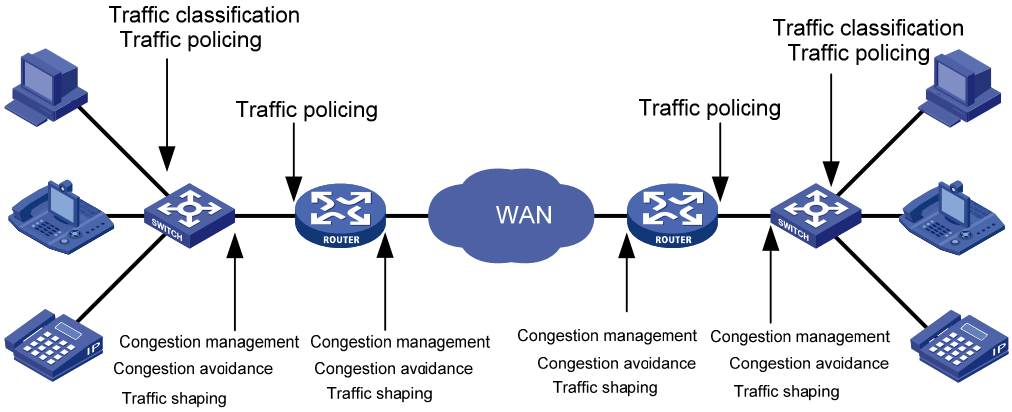
A simple solution for congestion is to increase network bandwidth. However, it cannot address all the problems of congestion.

A more effective solution is to provide differentiated services for different applications through traffic control and resource allocation. In this way, resources can be used more properly. During resources allocation and traffic control, the direct or indirect factors that might cause network congestion should be controlled to reduce the probability of congestion. Once congestion occurs, resource allocation should be performed according to the characteristics and demands of applications to minimize the effects of congestion on QoS.

# Major Traffic Management Techniques

## End-to-end QoS model

**Figure 1-2** End-to-end QoS model




As shown in Figure 1-2, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions:

- Traffic classification uses certain match criteria to organize packets with different characteristics into different classes, and is the prerequisite for providing differentiated services. Traffic classification is usually applied in the inbound direction of a port.
- Traffic policing polices particular flows entering a device according to configured specifications and is usually applied in the inbound direction of a port. When a flow exceeds the specification, some restriction or punishment measures can be taken to prevent overconsumption of network resources and protect the commercial benefits of the carrier.
- Traffic shaping proactively adjusts the output rate of traffic to adapt traffic to the network resources of the downstream device and avoid unnecessary packet drop and congestion. Traffic shaping is usually applied in the outbound direction of a port.
- Congestion management provides measures for handling resource competition during network congestion and is usually applied in the outbound direction of a port. Generally, it stores packets in queues, and then uses a scheduling algorithm to arrange the forwarding sequence of the packets.
- Congestion avoidance monitors the usage status of network resources and is usually applied in the outbound direction of a port. As congestion becomes worse, it actively reduces the amount of traffic by dropping packets.

Among these traffic management technologies, traffic classification is the basis for providing differentiated services by classifying packets with certain match criteria. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services.

This section is focused on traffic classification, and the subsequent sections will introduce the other technologies in details.

## Traffic Classification

Traffic classification organizes packets with different characteristics into different classes using match criteria. It is the basis for providing differentiated services.

You can define match criteria based on the IP precedence bits in the type of service (ToS) field of the IP packet header, or based on other header information such as IP addresses, MAC addresses, IP protocol field, and port numbers. Contents other than the header information in packets are rarely used for traffic classification. You can define a class for packets with a common quintuple (source address, source port number, protocol number, destination address and destination port number), or for all packets to a certain network segment.

When packets are classified at network boundaries, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be adopted as a classification criterion for the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream network can either inherit the classification results from its upstream network or re-classify the packets according to its own criteria.

To provide differentiated services, traffic classes must be associated with certain traffic control actions or resource allocation actions. What traffic control actions should be adopted depends on the current phase and the resources of the network. For example, CIR is adopted to police packets when they enter the network; generic traffic shaping (GTS) is performed on packets when they flow out of the node; queue scheduling is performed when congestion happens; congestion avoidance measures are taken when the congestion deteriorates.

# 2 QoS Policy Configuration

When configuring QoS policy, go to these sections for information that you are interested in:



## Overview

QoS policy includes the following three elements: class, traffic behavior and policy. You can bind the specified class to the specified traffic behavior through QoS policies to facilitate the QoS configuration.

### Class

Class is used for identifying traffic.

The elements of a class include the class name and classification rules.

You can use commands to define a series of rules to classify packets. Additionally, you can use commands to define the relationship among classification rules: “**and”** and “**or”**.

- **and**: The devices considers a packet to be of a specific class when the packet matches all the specified classification rules.
- **or**: The device considers a packet be of a specific class when the packet matches one of the specified classification rules.

### Traffic behavior

Traffic behavior is used to define all the QoS actions performed on packets.

The elements of a QoS behavior include traffic behavior name and actions defined in traffic behavior.

You can use commands to define multiple actions in a traffic behavior.

### Policy

Policy is used to bind the specified class to the specified traffic behavior.

The elements of a policy include the policy name and the name of the classification-to-behavior binding.

## Configuring a QoS Policy

The procedure for configuring QoS policy is as follows:

1) Define a class and define a group of traffic classification rules in class view.
2) Define a traffic behavior and define a group of QoS actions in traffic behavior view.
3) Define a policy and specify a traffic behavior corresponding to the class in policy view.

### Defining a Class

To define a class, you need to create a class and then define rules in the corresponding class view.

## Configuration procedure

Follow these steps to define a class:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a class and enter the corresponding class view | **traffic classifier** *classifier-name* [ **operator** { **and** \| **or** } ] | Required<br>By default, the **and** keyword is specified. That is, the relation between the rules in the class view is logic AND. This operation leads you to class view. |
| Define a rule used to match packets | **if-match** *match-criteria* | Required |

*match-criteria*: Matching rules to be defined for a class. Table 2-1 describes the available forms of this argument.

**Table 2-1** The form of the *match-criteria* argument

| Form | Description |
|---|---|
| **acl** *access-list-number* | Specifies an ACL to match packets. The access-list-number argument is in the range 2000 to 4999.<br>In a class configured with the operator **and**, the logical relationship between rules defined in the referenced IPv4 ACL is **or**. |
| **acl ipv6** *access-list-number* | Specifies an IPv6 ACL to match IPv6 packets. The access-list-number argument is in the range 2000 to 3999.<br>In a class configured with the operator **and**, the logical relationship between rules defined in the referenced IPv6 ACL is **or**. |
| **any** | Specifies to match all packets. |
| **customer-dot1p** *8021p-list* | Specifies to match packets by 802.1p precedence of the customer network. The *8021p-list* argument is a list of CoS values, in the range of 0 to 7.<br>**Note**<br>*Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4500G supports only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.* |
| **customer-vlan-id** *vlan-id-list* | Specifies to match the packets of specified VLANs of user networks. The *vlan-id-list* argument specifies a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094.<br>In a class configured with the operator **and**, the logical relationship between the customer VLAN IDs specified for the **customer-vlan-id** keyword is **or**. |
| **destination-mac** *mac-address* | Specifies to match the packets with a specified destination MAC address. |

| Form | Description |
|---|---|
| **dscp** *dscp-list* | Specifies to match packets by DSCP precedence. The *dscp-list* argument is a list of DSCP values in the range of 0 to 63.<br>**Note**<br>*Even though you can provide up to eight space-separated DSCP values for this argument, the Switch 4500G supports only one DSCP value in a rule. If you configure multiple DSCP values in a rule, the rule cannot be issued.* |
| **ip-precedence** *ip-precedence-list* | Specifies to match packets by IP precedence. The *ip-precedence-list* argument is a list of IP precedence values in the range of 0 to 7.<br>**Note**<br>*Even though you can provide up to eight space-separated IP precedence values for this argument, the Switch 4500G supports only one IP precedence value in a rule. If you configure multiple IP precedence values in a rule, the rule cannot be issued.* |
| **protocol** *protocol-name* | Specifies to match the packets of a specified protocol. The *protocol-name* argument can be IP or IPv6. |
| **service-dot1p** *8021p-list* | Specifies to match packets by 802.1p precedence of the service provider network. The *8021p-list* argument is a list of CoS values in the range of 0 to 7.<br>**Note**<br>*Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4500G supports only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.* |
| **service-vlan-id** *vlan-id-list* | Specifies to match the packets of the VLANs of the operator's network. The *vlan-id-list* argument is a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range of 1 to 4094.<br>In a class configured with the operator **and**, the logical relationship between the service VLAN IDs specified for the **service-vlan-id** keyword is **or**. |
| **source-mac** *mac-address* | Specifies to match the packets with a specified source MAC address. |

**Note**

Suppose the logical relationship between classification rules is **and**. Note the following when using the **if-match** command to define matching rules.

- If multiple matching rules with the **acl** or **acl ipv6** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.
- If multiple matching rules with the **customer-vlan-id** or **service-vlan-id** keyword specified are defined in a class, the actual logical relationship between these rules is **or**.

### Configuration example

1) Network requirements

Configure a class named test to match the packets with their IP precedence being 6.

2) Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Create the class. (This operation leads you to class view.)

```
[Sysname] traffic classifier test
```

# Define the classification rule.

```
[Sysname-classifier-test] if-match ip-precedence 6
```

## Defining a Traffic Behavior

To define a traffic behavior, you need to create a traffic behavior and then configure attributes for it in traffic behavior view.

### Configuration procedure

Follow these steps to define a traffic behavior:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a traffic behavior and enter the corresponding traffic behavior view | **traffic behavior** *behavior-name* | Required<br>*behavior-name*: Behavior name. This operation leads you to traffic behavior view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure accounting action | **accounting** | Required<br>You can configure the traffic behavior as required. |
| Configure traffic policing action | **car cir** *committed-information-rate* [ **cbs** *committed-burst-size* [ **ebs** *excess-burst-size* ] ] [ **pir** *peak-information-rate* ] [ **green** *action* ] [ **red** *action* ] [ **yellow** *action* ] | |
| Configure traffic filtering behavior | **filter** { **deny** \| **permit** } | |
| Configure traffic mirroring action | **mirror-to** { **cpu** \| **interface** *interface-type interface-number* } | |
| Configure traffic redirecting action | **redirect** { **cpu** \| **interface** *interface-type interface-number* \| **next-hop** { *ipv4-add* [ *ipv4-add* ] \| *ipv6-add* [ *interface-type interface-number* ] [ *ipv6-add* [ *interface-type interface-number* ] ] } } | |
| Remark DSCP value for packets | **remark dscp** *dscp-value* | |
| Remark 802.1p priority for packets | **remark dot1p** *8021p* | |
| Remark drop precedence for packets | **remark drop-precedence** *drop-precedence-value* | |
| Remark IP precedence for packets | **remark ip-precedence** *ip-precedence-value* | |
| Remark local precedence for packets | **remark local-precedence** *local-precedence* | |

### Configuration example

1) Network requirements

Create a traffic behavior named test, configuring traffic policing action for it, with the CAR being 640 kbps.

2) Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Create the traffic behavior (This operation leads you to traffic behavior view).

```
[Sysname] traffic behavior test
```

# Configure traffic policing action for the traffic behavior.

```
[Sysname-behavior-test] car cir 640
```

## Defining a Policy

A policy associates a class with a traffic behavior. Each traffic behavior is comprised of a group of QoS actions. A device executes these QoS actions in the order they are defined.

Follow these steps to associate a traffic behavior with a class:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a policy (This operation leads you to policy view) | **qos policy** *policy-name* | — |
| Specify the traffic behavior for a class | **classifier** *classifier-name* **behavior** *behavior-name* | Required |

## Applying a Policy

You can apply a QoS policy in different views as follows:

- In port or port group view, the policy applies to the inbound or outbound direction of an interface or a group of interfaces;
- In user profile view, the policy applies to the traffic sent or received by the online users;
- In VLAN view, the policy applies to the inbound or outbound direction of a VLAN;

**Note**

- You cannot modify the classification rules, traffic behaviors, and classifier-behavior associations in a QoS policy already applied. To check whether a QoS policy has been applied successfully, use the **display qos policy global** command and the **display qos policy interface** command.
- The switch may save the applications of some QoS policies that have failed to be applied due to insufficient hardware resources in the configuration file. After the switch reboots, these policies may preempt other user configurations for resources, resulting in loss of configurations. Suppose that the **user-bind** command is configured on GigabitEthernet 1/0/2, and the application of a QoS policy to GigabitEthernet 1/0/1 is saved in the configuration file even though the application has failed due to insufficient resources. After the switch reboots, it may assign resources to have the QoS policy take effect preferentially, while the **user-bind** configuration may be lost due to insufficient resources.

### Applying a QoS policy to a port/port group

A policy can be applied to multiple ports. Only one policy can be applied in inbound direction of a port/port group.

Follow these steps to apply the QoS policy to a port/port group:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Apply an associated policy | **qos apply policy** *policy-name* **inbound** | Required |

### Applying a QoS policy to online users

You can apply a QoS policy to traffic of multiple online users. You can apply only one policy in one direction (inbound or outbound) of the traffic of online users. To modify a QoS policy already applied, remove the QoS policy application first.

Follow these steps to apply a QoS policy to traffic of online users:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter user profile view | **user-profile** *profile-name* **dot1x** | Required<br>The configuration made in user profile view takes effect when the user-profile is active and the corresponding users are online. |
| Apply the QoS policy | **qos apply policy** *policy-name* { **inbound** \| **outbound** } | Required |
| Return to system view | **quit** | — |
| Activate the user profile | **user-profile** *profile-name* **enable** | Required<br>Inactive by default. |

**Note**

- When a user profile is active, you cannot configure or remove the QoS policy applied to it.
- The QoS policies applied in user profile view support only the **remark**, **car**, and **filter** actions.
- Do not apply an empty QoS policy in user profile view, because even if you can do that, the user profile cannot be activated.
- Refer to *User Profile Configuration* in the *QoS Volume* for more information about user profiles.

### Applying a QoS policy to a VLAN

Follow these steps to apply the QoS policy to a VLAN:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Apply the QoS policy to the specified VLAN(s) | **qos vlan-policy** *policy-name* **vlan** *vlan-id-list* **inbound** | Required |

**Note**

- QoS policies cannot be applied to dynamic VLANs, for example, VLANs created by GVRP.
- Do not apply a QoS policy to a VLAN and the ports in the VLAN at the same time.

### Configuration example

1) Configuration example 1

Configure a QoS policy **test_policy**. Associate the traffic behavior **test_behavior** with the traffic class **test_class** in the policy, and apply the policy to:

- the inbound direction of GigabitEthernet 1/0/1.
- the inbound direction of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.

Configuration procedure:

# Enter system view.

```
<Sysname> system-view
```

# Create a policy (This operation leads you to policy view).

```
[Sysname] qos policy test_policy
[Sysname-qospolicy-test_policy]
```

# Associate the traffic behavior **test_behavior** with the class **test_class**.

```
[Sysname-qospolicy-test_policy] classifier test_class behavior test_behavior
[Sysname-qospolicy-test_policy] quit
```

# Apply the QoS policy to the inbound direction of GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy test_policy inbound
[Sysname-GigabitEthernet1/0/1] quit
```

# Apply the QoS policy to the inbound direction of the specified VLANs.

```
[Sysname] qos vlan-policy test_policy vlan 200 300 400 500 600 700 800 900 inbound
```

2) Configuration example 2

# Apply the QoS policy **test_policy** in the inbound direction of the online users of the 802.1x user profile **user**.

```
<Sysname> system-view
[Sysname] user-profile user dot1x
[Sysname-user-profile-DOT1X-user] qos apply policy test_policy inbound
[Sysname-user-profile-DOT1X-user] quit
[Sysname] user-profile user enable
```

## Displaying and Maintaining QoS Policies

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about a class and the corresponding actions associated by a policy | **display qos policy user-defined** [ *policy-name* [ **classifier** *classifier-name* ] ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about the policies applied on a port | **display qos policy interface** [ *interface-type interface-number* ] [ **inbound** ] | Available in any view |
| Display information about a traffic behavior | **display traffic behavior user-defined** [ *behavior-name* ] | Available in any view |
| Display information about a class | **display traffic classifier user-defined** [ *classifier-name* ] | Available in any view |
| Display information about QoS policies applied to VLANs | **display qos vlan-policy** { **name** *policy-name* \| **vlan** [ *vlan-id* ] } [ **inbound** ] | Available in any view |
| Clear the statistics of QoS policies applied to VLANs | **reset qos vlan-policy** [ **vlan** *vlan-id* ] [ **inbound** ] | Available in user view |

# 3 Priority Mapping

When configuring priority mapping, go to these sections for information you are interested in:

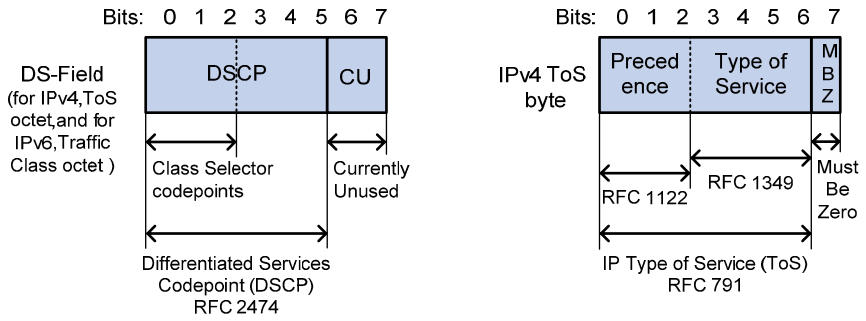


## Priority Overview

The following describes several types of precedence:

1) IP precedence, ToS precedence, and DSCP precedence

**Figure 3-1** DS field and ToS field




The ToS field in an IP header contains eight bits, which are described as follows:

- The first three bits indicate IP precedence in the range of 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- RFC2474 re-defines the ToS field in the IP packet header, which is called the DS field. The first six (bit 0 to bit 5) bits of the DS field indicate DSCP precedence in the range of 0 to 63. The last two bits (bit 6 and bit 7) are reserved bits.

**Table 3-1** Description on IP Precedence

| IP Precedence (decimal) | IP Precedence (binary) | Description |
|---|---|---|
| 0 | 000 | Routine |
| 1 | 001 | priority |
| 2 | 010 | immediate |
| 3 | 011 | flash |
| 4 | 100 | flash-override |
| 5 | 101 | critical |

| IP Precedence (decimal) | IP Precedence (binary) | Description |
|---|---|---|
| 6 | 110 | internet |
| 7 | 111 | network |

In a network providing differentiated services, traffics are grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential services with low delay, low packet loss ratio, low jitter, and assured bandwidth (such as virtual leased line);
- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;
- Class selector (CS) class: This class comes from the IP ToS field and includes eight subclasses;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

**Table 3-2** Description on DSCP precedence values

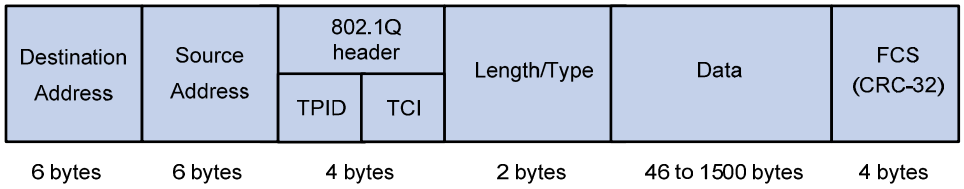
| DSCP value (decimal) | DSCP value (binary) | Description |
|---|---|---|
| 46 | 101110 | ef |
| 10 | 001010 | af11 |
| 12 | 001100 | af12 |
| 14 | 001110 | af13 |
| 18 | 010010 | af21 |
| 20 | 010100 | af22 |
| 22 | 010110 | af23 |
| 26 | 011010 | af31 |
| 28 | 011100 | af32 |
| 30 | 011110 | af33 |
| 34 | 100010 | af41 |
| 36 | 100100 | af42 |
| 38 | 100110 | af43 |
| 8 | 001000 | cs1 |
| 16 | 010000 | cs2 |
| 24 | 011000 | cs3 |
| 32 | 100000 | cs4 |
| 40 | 101000 | cs5 |
| 48 | 110000 | cs6 |

| DSCP value (decimal) | DSCP value (binary) | Description |
|---|---|---|
| 56 | 111000 | cs7 |
| 0 | 000000 | be (default) |

2) 802.1p priority

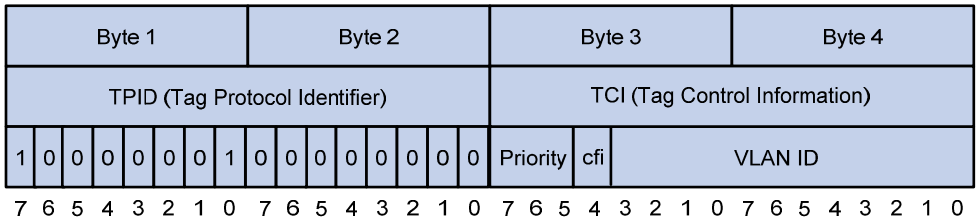
802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2.

**Figure 3-2** An Ethernet frame with an 802.1Q tag header




As shown in Figure 3-2, the 4-byte 802.1Q tag header contains a 2-byte Tag Protocol Identifier (TPID) whose value is 8100 and a 2-byte Tag Control Information (TCI). TPID is a new class defined by IEEE to indicate a packet with an 802.1Q tag. Figure 3-3 describes the detailed contents of an 802.1Q tag header.

**Figure 3-3** 802.1Q tag header




In the figure above, the 3-bit priority field in TCI is 802.1p priority in the range of 0 to 7. In the figure above, the priority field (three bits in length) in TCI is 802.1p priority (also known as CoS precedence), which ranges from 0 to 7.

**Table 3-3** Description on 802.1p priority

| 802.1p priority (decimal) | 802.1p priority (binary) | Description |
|---|---|---|
| 0 | 000 | best-effort |
| 1 | 001 | background |
| 2 | 010 | spare |
| 3 | 011 | excellent-effort |
| 4 | 100 | controlled-load |
| 5 | 101 | video |
| 6 | 110 | voice |
| 7 | 111 | network-management |

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

## Priority Mapping Overview

When a packet reaches a switch, the switch assigns the packet parameters according to it configuration, such as 802.1p precedence, DSCP precedence, IP precedence, local precedence, and drop precedence.

The local precedence and drop precedence are described as follows.

- Local precedence is the precedence that the switch assigns to a packet and it is corresponding to the number of an outbound queue on the port. Local precedence takes effect only on the local switch.
- Drop precedence is a parameter that is referred to when dropping packets. The higher the drop precedence, the more likely a packet is dropped.

Depending on whether a received packet is 802.1q-tagged, the switch marks it with priority as follows:

1) For an 802.1q-untagged packet

When a packet carrying no 802.1q tag reaches a port, the switch uses the port priority as the 802.1p precedence value of the received packet, searches for the local precedence value corresponding to the port priority of the receiving port in the 802.1p-precedence-to-local-precedence mapping table, assigns the local precedence value to the packet, and enqueues the packet according to the local precedence value.

2) For an 802.1q-tagged packet

When an 802.1q tagged packet reaches the port of a switch, you can specify a priority trust mode for the port, trusting port priority or trusting packet priority.

- Trusting packet priority

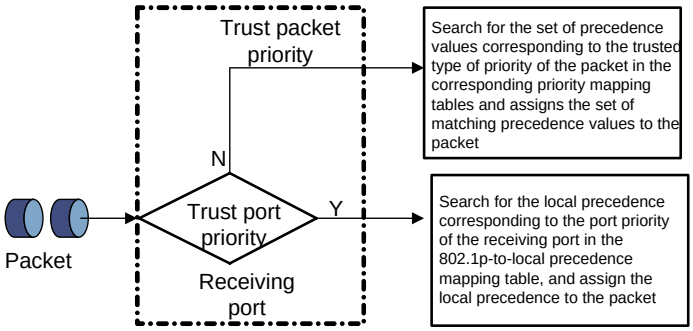
In this mode, the switch searches for the set of precedence values corresponding to the trusted type (802.1p precedence or DSCP precedence) of priority of the packet in the corresponding priority mapping tables and assigns the set of matching precedence values to the packet.

- Trusting port priority

In this mode, the switch replaces the 802.1p priority of the received packet with the port priority, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, assigns the local precedence to the packet, and enqueues the packet according to the local precedence value.

You can configure the priority trust mode of a port as required. The priority mapping process on a switch is as shown in Figure 3-4.

**Figure 3-4** Priority mapping process in the case of supporting trusting port priority




When trusting packet priority, Switch 4500G series Ethernet switches provide the following two priority trust modes:can trust one of the following two priority types:

- Trusting the DSCP precedence of received packets. In this mode, the switch searches the **dscp-dot1p/dp/dscp** mapping table based on the DSCP precedence of the received packet for the 802.1p precedence/drop precedence/DSCP precedence to be used to mark the packet. Then the switch searches the **dot1p-lp** mapping table based on the marked 802.1p precedence for the corresponding local precedence and marks the received packet with the local precedence.
- Trusting the 802.1p precedence of received packets. In this mode, if a packet is received without an 802.1q tag, the switch takes the priority of the receiving port as the 802.1p precedence of the packet and then based on the priority searches the **dot1p-dp/lp** mapping table for the local/drop precedence for the packet. If packet is received with an 802.1q tag, the switch searches the **dot1p-dp/lp** mapping table based on the 802.1p precedence in the tag for local/drop precedence for the packet.

The default **dot1p-lp/dp** mapping and **dscp-dot1p/dp/dscp** mapping provided by Switch 4500G series Ethernet switches are shown in the following two tables.

- **dot1p-dp**: 802.1p-priority-to-drop-precedence mapping table
- **dot1p-lp**: 802.1p-priority-to-local-precedence mapping table
- **dscp-dot1p**: DSCP-precedence-to-802.1p-priority mapping table
- **dscp-dp**: DSCP-precedence-to-drop-precedence mapping table, applicable to only IP packets
- **dscp-dscp**: DSCP-precedence-to-DSCP-precedence mapping table, applicable to only IP packets

**Table 3-4** The default values of **dot1p-lp** mapping and **dot1p-dp** mapping

| Imported priority value | dot1p-lp mapping | dot1p-dp mapping |
|---|---|---|
| 802.1p precedence (**dot1p**) | Local precedence (**lp**) | Drop precedence (**dp**) |
| 0 | 2 | 0 |
| 1 | 0 | 0 |
| 2 | 1 | 0 |
| 3 | 3 | 0 |
| 4 | 4 | 0 |
| 5 | 5 | 0 |
| 6 | 6 | 0 |
| 7 | 7 | 0 |

**Table 3-5** The default values of **dscp-dp** mapping, **dscp-dot1p** mapping, and **dscp-dscp** mapping

| Imported priority value | dscp-dp mapping | dscp-dot1p mapping | dscp-dscp mapping |
|---|---|---|---|
| DSCP precedence (**dscp**) | Drop precedence (**dp**) | 802.1p precedence (**dot1p**) | DSCP precedence (**dscp**) |
| 0 to 7 | 0 | 0 | 0 to 7 |
| 8 to 15 | 0 | 1 | 8 to 15 |
| 16 to 23 | 0 | 2 | 16 to 23 |
| 24 to 31 | 0 | 3 | 24 to 31 |
| 32 to 39 | 0 | 4 | 32 to 39 |
| 40 to 47 | 0 | 5 | 40 to 47 |
| 48 to 55 | 0 | 6 | 48 to 55 |
| 56 to 63 | 0 | 7 | 56 to 63 |

# Configuring a Priority Mapping Table

You can modify the priority mapping tables in a switch as required.

Follow the two steps to configure priority mapping tables:

- Enter priority mapping table view;
- Configure priority mapping parameters.

## Configuration Prerequisites

The new priority mapping table is determined.

## Configuration Procedure

Follow these steps to configure a priority mapping table:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter priority mapping table view | **qos map-table** { **dot1p-dp** \| **dot1p-lp** \| **dscp-dot1p** \| **dscp-dp** \| **dscp-dscp** } | Required<br>To configure a priority mapping table, you need to enter the corresponding priority mapping table view. |
| Configure priority mapping parameters | **import** *import-value-list* **export** *export-value* | Required<br>The newly configured mapping entries overwrite the corresponding previous entries. |

**Note**

You cannot configure to map any DSCP value to drop precedence 1.

## Configuration Example

### Network requirements

Modify the **dot1p-lp** mapping table as those listed in Table 3-6.

**Table 3-6** The specified **dot1p-lp** mapping

| 802.1p precedence | Local precedence |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 2 | 1 |
| 3 | 1 |
| 4 | 2 |
| 5 | 2 |
| 6 | 3 |
| 7 | 3 |

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Enter **dot1p-lp** priority mapping table view.

```
[Sysname] qos map-table dot1p-lp
```

# Modify **dot1p-lp** priority mapping parameters.

```
[Sysname-maptbl-dot1p-lp] import 0 1 export 0
[Sysname-maptbl-dot1p-lp] import 2 3 export 1
[Sysname-maptbl-dot1p-lp] import 4 5 export 2
[Sysname-maptbl-dot1p-lp] import 6 7 export 3
```

# Configuring the Port Priority

By default, if a port receives packets without 802.1q tags, the switch takes the priority of the receiving port as the 802.1p precedence of the received packets, searches the **dot1p-lp/dp** mapping table for the corresponding local precedence and drop precedence according to the 802.1p precedence of the received packets, and then marks the received packets with the corresponding local precedence and drop precedence.

Port priority is in the range 0 to 7. You can set the port priority as required.

## Configuration Prerequisites

The port priority of the port is determined.

## Configuration Procedure

Follow these steps to configure port priority:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure port priority | | **qos priority** *priority-value* | Required<br>By default, the port priority is 0. |

## Configuration Example

### Network requirements

Configure the port priority to 7.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Configure port priority of GigabitEthernet1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 7
```

# Configuring Port Priority Trust Mode

You can configure the switch to trust the DSCP precedence of the received packets. In this case, the switch searches the **dscp-dot1p/dp/dscp** mapping table for the corresponding precedence according to the DSCP precedence of the packets and marks the received packets with the precedence.

## Configuration Prerequisites

It is determined to trust the DSCP precedence or the 802.1p precedence of received packets.

## Configuration Procedure

Follow these steps to configure the port priority trust mode:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure to trust the DSCP precedence or the 802.1p precedence of the received packets | | **qos trust** { **dscp** \| **dot1p** } | Perform either of the two operations.<br>By default, the port priority is trusted. |
| Configure to trust the port priority | | **undo qod trust** | |

## Configuration Example

### Network requirements

Configure to trust the DSCP precedence of the received packets.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Enter port view.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

# Configure to trust the DSCP precedence of the received packets.

```
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

# Displaying and Maintaining Priority Mapping

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the information about a specified priority mapping table | **display qos map-table** [ **dot1p-dp** \| **dot1p-lp** \| **dscp-dot1p** \| **dscp-dp** \| **dscp-dscp** ] | Available in any view |
| Display the priority trust mode configured for a port | **display qos trust interface** [ *interface-type interface-number* ] | |

# 4 Traffic Policing and Line Rate Configuration

When configuring traffic classification, traffic policing, traffic shaping, and line rate, go to these section for information you are interested in:



## Traffic Policing and Line Rate Overview

If the traffic from users is not limited, a large amount of continuous burst packets will result in worse network congestion. The traffic of users must be limited in order to make better use of the limited network resources and provide better service for more users. For example, if a traffic flow obtains only the resources committed to it within a certain period of time, network congestion due to excessive burst traffic can be avoided.

- Traffic policing is a traffic control policie for limiting traffic and resource usage by supervising the traffic. The prerequisite for traffic policing is to determine whether or not the traffic exceeds the set threshold. Traffic control policies are adopted only when the traffic exceeds the set threshold. Generally, token bucket is used for evaluating traffic.
- The line rate of a physical interface specifies the maximum rate for forwarding packets. Line rate also uses token buckets for traffic control.

### Traffic Evaluation and the Token Bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

#### Evaluating traffic with the token bucket

The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets, the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess.

When the token bucket evaluates the traffic, its parameter configurations include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is generally set to committed burst size (CBS). The set burst size must be greater than the maximum packet length.

An evaluation is performed on the arrival of each packet. In each evaluation, if the bucket has enough tokens for use, the traffic is controlled within the specification and a number of tokens equivalent to the packet forwarding authority must be taken out; otherwise, this means too many tokens have been used — the traffic is in excess of the specification.

### Complicated Evaluation

You can set two token buckets (referred to as the C bucket and E bucket respectively) in order to evaluate more complicated conditions and implement more flexible regulation policies. For example, traffic policing uses four parameters:

- CIR: Rate at which tokens are put into the C bucket, that is, the average packet transmission or forwarding rate allowed by the C bucket.
- CBS: Size of the C bucket, that is, transient burst of traffic that the C bucket can forward.
- Peak information rate (PIR): Rate at which tokens are put into the E bucket, that is, the average packet transmission or forwarding rate allowed by the E bucket.
- Excess burst size (EBS): Size of the E bucket, that is, transient burst of traffic that the E bucket can forward.

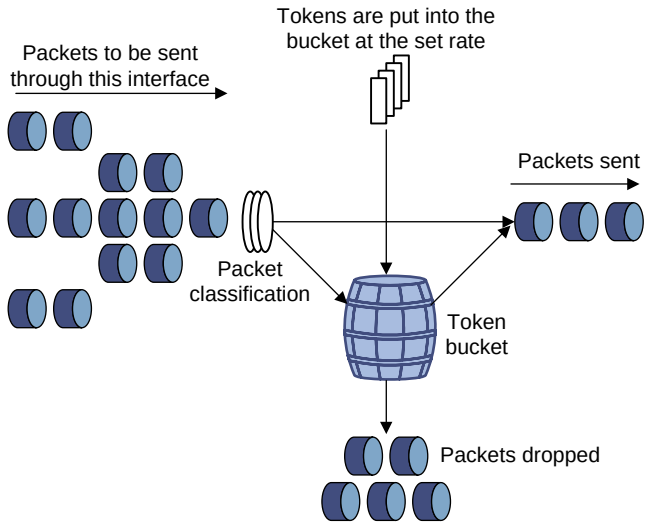
In each evaluation, packets are measured against the buckets:

- If the C bucket has enough tokens, packets are colored green.
- If the C bucket does not have enough tokens but the E bucket has enough tokens, packets are colored yellow.
- If neither the C bucket nor the E bucket has sufficient tokens, packets are colored red.

## Traffic Policing

The typical application of traffic policing is to supervise the specification of certain traffic into the network and limit it within a reasonable range, or to "discipline" the extra traffic. In this way, the network resources and the interests of the operators are protected. For example, you can limit HTTP packets to be within 50% of the network bandwidth. If the traffic of a certain connection is excess, traffic policing can choose to drop the packets or to reset the priority of the packets.

**Figure 4-1** Diagram for TP




Traffic policing is widely used in policing the traffic into the network of internet service providers (ISPs). Traffic policing can classify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

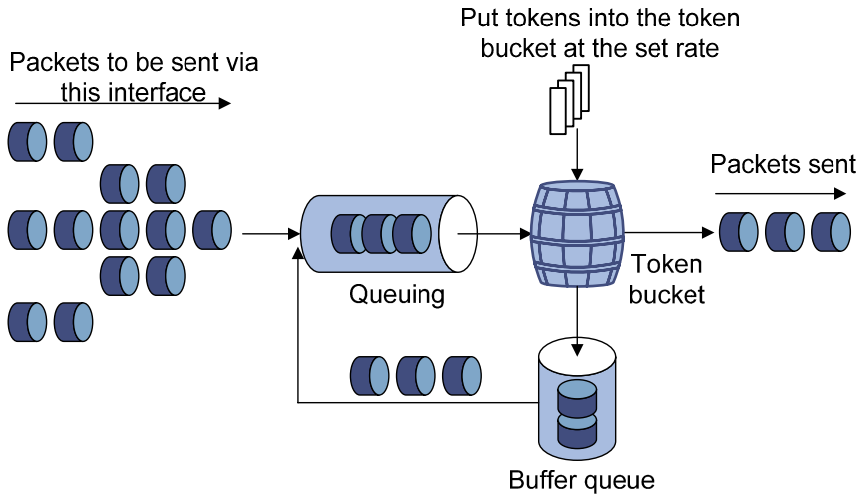
- Forwarding conforming packets or non-conforming packets.
- Dropping conforming or non-conforming packets.
- Marking a conforming packet or a non-conforming packet with a new DSCP precedence value and forwarding the packet.

## Line Rate

The line rate of a physical interface specifies the maximum rate for forwarding packets (including critical packets).

Line rate also uses token buckets for traffic control. With line rate configured on an interface, all packets to be sent through the interface are first handled by the token bucket at line rate. If there are enough tokens in the token bucket, packets can be forwarded; otherwise, packets are put into QoS queues for congestion management. In this way, the traffic passing the physical interface is controlled.

**Figure 4-2** Line rate implementation




In the token bucket approach to traffic control, burst traffic can be transmitted so long as enough tokens are available in the token bucket; if tokens are inadequate, packets cannot be transmitted until the required number of tokens are generated in the token bucket. Thus, traffic rate is restricted to the rate for generating tokens, thus limiting traffic rate and allowing bursty traffic.

Compared with traffic policing, line rate can only limit traffic rate on a physical interface. Since traffic policing operates at the IP layer, it can limit the rate of different flows on a port. However, traffic policing ignores packets not processed by the IP layer. To limit the rate of all the packets on interfaces, using line rate is easier.

# CAR/Line Rate Configuration

**Note**

On the Switch 4500G series switches, traffic policing is achieved mainly through QoS policies. For QoS policy configuration, refer to Configuring a QoS Policy.

## Line Rate Configuration Procedure

### Configuration procedure

Follow these steps to configure line rate:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter interface view or port group view | Enter port view | **interface** *interface-type interface-number* | Enter either view.<br>Settings in interface view take effect on the current interface; settings in port group view take effect on all ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure line rate | | **qos lr outbound cir** *committed-information-rate* [ **cbs** *committed-burst-size* ] | Required |

### Line rate configuration examples

Limit the outbound rate of GigabitEthernet 1/0/1 to 640 kbps.

# Enter system view.

```
<Sysname> system-view
```

# Enter interface view.

```
[Sysname] interface GigabitEthernet 1/0/1
```

# Configure line rate parameter and limit the outbound rate to 640 kbps.

```
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

## Displaying Line Rate

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the line rate configuration of interfaces | **display qos lr interface** [ *interface-type interface-number* ] | Available in any view |

# 5 Congestion Management

When configuring congestion management, go to these section for information that you are interested in:



## Overview

When the rate at which the packets arrive is higher than the rate at which the packets are transmitted on an interface, congestion occurs on this interface. If there is not enough storage space to store these packets, parts of them will be lost. Packet loss may cause the transmitting device to retransmit the packets because the lost packets time out, which causes a malicious cycle.

The core of congestion management is how to schedule the resources and determine the sequence of forwarding packets when congestion occurs. Congestion management processing includes queue creating, traffic classification, packet enqueuing, and queue scheduling.

## Congestion Management Policy

Queuing technology is generally adopted to solve the congestion problem. The queuing technology is to classify the traffic according to a specified queue-scheduling algorithm and then use the specified priority algorithm to forward the traffic. Each queuing algorithm is used to solve specific network traffic problems and affects the parameters such as bandwidth allocation, delay and delay jitter.

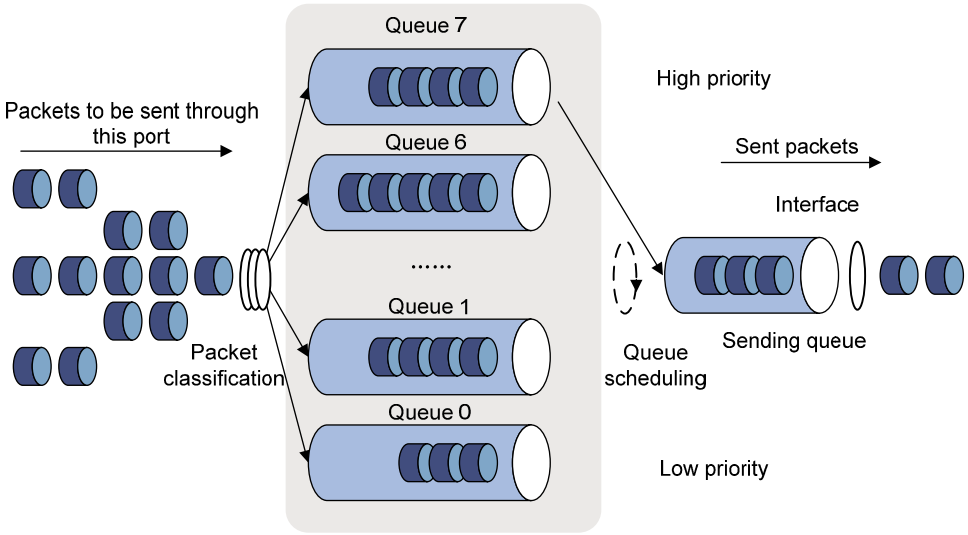
The Switch 4500G series support the following four queue scheduling methods:

- Scheduling all queues with the strict priority (SP) algorithm.
- Scheduling all queues with the weighted round robin (WRR) algorithm.
- Scheduling all queues with the weighted fair queuing (WFQ) algorithm
- Scheduling some queues with the SP algorithm and some with the WRR algorithm.

This section describe how SP, WRR, WFQ, and SP+WRR work in details.

1) SP queue-scheduling algorithm

**Figure 5-1** Diagram for SP queuing



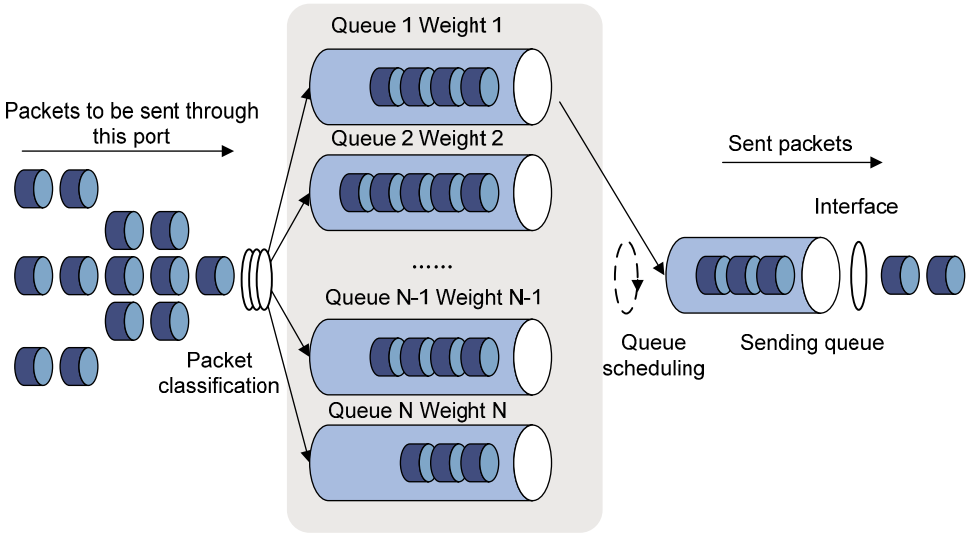

SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

2) WRR queue-scheduling algorithm

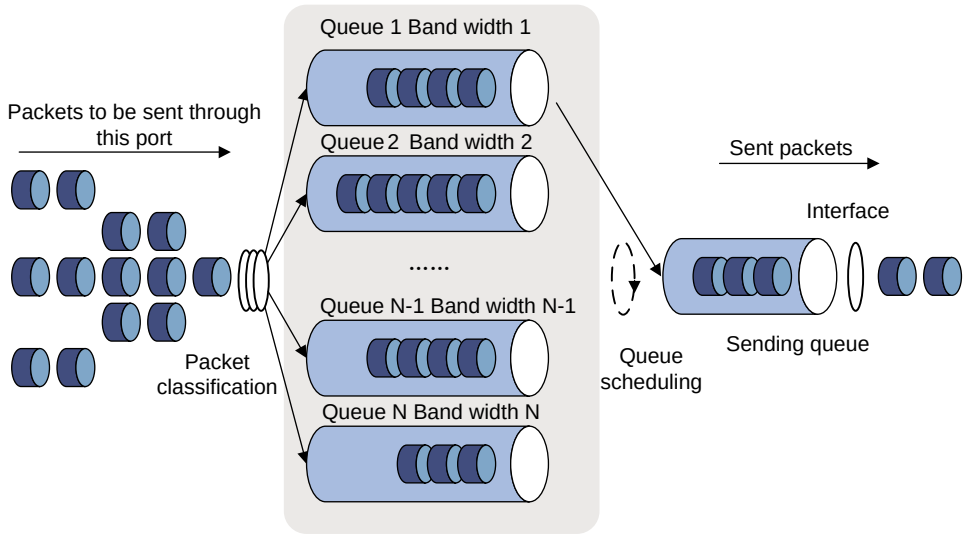
**Figure 5-2** Diagram for WRR queuing



A port of the switch supports eight outbound queues. The WRR queue-scheduling algorithm schedules all the queues in turn to ensure that every queue can be assigned a certain service time. Assume there are eight output queues on the port. The eight weight values (namely, w 7, w 6, w 5, w 4, w 3, w 2, w 1, and w 0) indicating the proportion of assigned resources are assigned to the eight queues respectively. On a 100M port, you can configure the weight values of WRR queue-scheduling algorithm to 50, 30, 10, 10, 50, 30, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 respectively). In this way, the queue with the lowest priority can be assured of 5 Mbps of bandwidth at least, thus avoiding the disadvantage of SP queue-scheduling algorithm that packets in low-priority queues are possibly not to be served for a long time. Another advantage of WRR queue-scheduling algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled immediately. In this way, the bandwidth resources are fully utilized.

3) WFQ queue-scheduling algorithm

**Figure 5-3** Diagram for WFQ queuing




Before WFQ is introduced, you need to understand fair queuing (FQ). FQ is designed for fairly sharing network resources, reducing the delay and jitter of all traffic. FQ takes all the aspects into consideration:

- Different queues have fair dispatching opportunities for delay balancing among streams.
- Short packets and long packets are fairly scheduled: if there are long packets and short packets in queues, statistically the short packets should be scheduled preferentially to reduce the jitter between packets on the whole.

Compared with FQ, WFQ takes weights into account when determining the queue scheduling order. Statistically, WFQ gives high priority traffic more scheduling opportunities than low priority traffic. WFQ can automatically classify traffic according to the “session” information of traffic (protocol type, TCP or UDP source/destination port numbers, source/destination IP addresses, IP precedence bits in the ToS field, etc), and try to provide as many queues as possible so that each traffic flow can be put into these queues to balance the delay of every traffic flow on a whole. When dequeuing packets, WFQ assigns the outgoing interface bandwidth to each traffic flow by the precedence. The higher precedence value a traffic flow has, the more bandwidth it gets.

The Switch 4500G series switches introduce the minimum guaranteed bandwidth mechanism, and use it in conjunction with WFQ as follows:

- The minimum guaranteed bandwidth configuration guarantees a certain amount of bandwidth for each WFQ queue.

- The allocable bandwidth (allocable bandwidth = the total bandwidth – the sum of the minimum guaranteed bandwidth for each queue) is divided and allocated to each queue based on queue precedence.

For example, assume that the total bandwidth of an interface is 10 Mbps and there are five flows on the interface, with the precedence being 0, 1, 2, 3, and 4 respectively and the minimum guaranteed bandwidth being 128 kbps, 128 kbps, 128 kbps, 64 kbps, and 64 kbps respectively. Then,

- The allocable bandwidth = 10 Mbps – (128 + 128 + 128 + 64 + 64) kbps = 9.5 Mbps
- The total allocable bandwidth quota is the sum of all the (precedence value + 1)s, that is, 1 + 2 + 3 + 4 + 5 = 15.
- The bandwidth percentage assigned to each flow is (precedence value of the flow + 1)/total allocable bandwidth quota. The bandwidth percentages for flows are 1/15, 2/15, 3/15, 4/15, and 5/15 respectively.
- The bandwidth allocated to a queue = Minimum guaranteed bandwidth + bandwidth allocated to the queue from the allocable bandwidth

Because WFQ can balance the delay and jitter of every flow when congestion occurs, it is effectively applied in some special occasions. For example, WFQ is adopted in the assured forwarding (AF) services of the Resource Reservation Protocol (RSVP). In Generic Traffic Shaping (GTS), WFQ is used to schedule buffered packets.

4) SP+WRR queue scheduling algorithm

You can implement SP+WRR queue scheduling on a port by assigning some queues on the port to the SP scheduling group and the others to the WRR scheduling group (that is, group 1). Packets in the SP scheduling group are scheduled preferentially. When the SP scheduling group is empty, packets in the WRR scheduling group are scheduled. Queues in the SP scheduling group are scheduled by SP. Queues in the WRR scheduling group are scheduled by WRR.

# Configuring an SP Queue

By default, WRR queue scheduling algorithm is adopted on all the ports. You can adopt SP queue scheduling algorithm instead as required.

## Configuration Procedure

Follow these steps to configure SP queues:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Configure SP queue scheduling algorithm | | **qos sp** | Required<br>By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15. |

## Configuration Example

### Network requirements

Configure GigabitEthernet1/0/1 to adopt SP queue scheduling algorithm.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Configure an SP queue for GigabitEthernet1/0/1 port.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

# Configuring a WRR Queue

## Configuration Procedure

Follow these steps to configure WRR queues:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable WRR on the port | | **qos wrr** | Optional<br>Enabled by default. |
| Configure WRR queue scheduling | | **qos wrr** *queue-id* **group** *group-id* **weight** *schedule-value* | Required<br>By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15. |

## Configuration Example

### Network requirements

Configure WRR queue scheduling algorithm on GigabitEthernet1/0/1, and assign weight 1, 2, 4, 6, 8, 10, 12, and 14 to queue 0 through queue 7.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Configure the WRR queues on GigabitEthernet1/0/1 port.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 1
```

```
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 1 weight 4
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 1 weight 6
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 weight 8
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 weight 10
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 weight 12
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 weight 14
```

# Configuring a WFQ Queue

By default, all ports adopt the WRR queue algorithm. You can configure a port to use the WFQ algorithm instead as required.

## Configuration Procedure

Follow these steps to configure WFQ queues:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Adopt the WFQ queue scheduling on the port | | **qos wfq** | Required<br>By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15. |
| Configure the minimum guaranteed bandwidth for a WFQ queue | | **qos bandwidth queue** *queue-id* **min** *bandwidth-value* | Optional<br>By default, the minimum guaranteed bandwidth of a queue is 64 kbps. |
| Configure a scheduling weight for the specified queue | | **qos wfq** *queue-id* **weight** *schedule-value* | Optional<br>By default, the scheduling weight of a WFQ queue is 1. |

## Configuration Example

### Network requirements

Enable WFQ on GigabitEthernet 1/0/1 and assign weight values 1, 2, 4, 6, 8, 10, 12, and 14 to queues 0 through 7 respectively.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Configure the WFQ queues on GigabitEthernet1/0/1 port.

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 0 weight 1
[Sysname-GigabitEthernet1/0/1] qos wfq 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wfq 2 weight 4
[Sysname-GigabitEthernet1/0/1] qos wfq 3 weight 6
[Sysname-GigabitEthernet1/0/1] qos wfq 4 weight 8
[Sysname-GigabitEthernet1/0/1] qos wfq 5 weight 10
[Sysname-GigabitEthernet1/0/1] qos wfq 6 weight 12
[Sysname-GigabitEthernet1/0/1] qos wfq 7 weight 14
```

# Configuring SP+WRR Queues

By default, all ports adopt the WRR queue algorithm. You can configure a port to use the SP+WRR queue scheduling algorithm as required.

## Configuration Procedure

Follow these steps to configure SP + WRR queues:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter port view or port group view | Enter port view | **interface** *interface-type interface-number* | Perform either of the two operations.<br>The configuration performed in Ethernet interface view applies to the current port only. The configuration performed in port group view applies to all the ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| Enable the WRR queue scheduling on the port | | **qos wrr** | Required |
| Configure SP queue scheduling | | **qos wrr** *queue-id* **group sp** | Required<br>By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15. |
| Configure WRR queue scheduling | | **qos wrr** *queue-id* **group** *group-id* **weight** *schedule-value* | Required<br>By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15. |

## Configuration Example

### Network requirements

- Configure to adopt SP+WRR queue scheduling algorithm on GigabitEthernet1/0/1.
- Configure queue 0, queue 1, queue 2 and queue 3 on GigabitEthernet1/0/1 to be in SP queue scheduling group.
- Configure queue 4, queue 5, queue 6 and queue 7 on GigabitEthernet1/0/1 to be in WRR queue scheduling group, with the weight being 2, 4, 6 and 8 respectively.

### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Enable the SP+WRR queue scheduling algorithm on GigabitEthernet1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 weight 4
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 weight 6
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 weight 8
```

## Displaying and Maintaining Congestion Management

| To do… | Use the command… | Remarks |
|---|---|---|
| Display WRR queue configuration information | **display qos wrr interface** [ *interface-type interface-number* ] | Available in any view |
| Display SP queue configuration information | **display qos sp interface** [ *interface-type interface-number* ] | |
| Display WFQ queue configuration information | **display qos wfq interface** [ *interface-type interface-number* ] | |

# 6 Traffic Mirroring Configuration

When configuring traffic mirroring, go to these sections for information that you are interested in:



## Overview

Traffic mirroring is to replicate the specified packets to the specified destination. It is generally used for testing and troubleshooting the network. .

Depending on different types of mirroring destinations, there are three types of traffic mirroring:

- Mirroring to port: The desired traffic on a mirrored port is replicated and sent to a destination port (that is, a mirroring port).
- Mirroring to CPU: The desired traffic on a mirrored port is replicated and sent to the CPU for further analysis.
- Mirroring to VLAN: The desired traffic on a mirrored port is replicated and sent to a VLAN, where the traffic is broadcast and all the ports (if available) in the VLAN will receive the traffic. If the destination VLAN does not exist, you can still configure the function, and the function will automatically take effect after the VLAN is created and a port is added to it.

**Note**

On Switch 4500G series Ethernet switches, traffic can only be mirrored to ports and to CPU.

## Configuring Traffic Mirroring

To configure traffic mirroring, you must enter the view of an existing traffic behavior.

Follow these steps to configure traffic mirroring to a port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter traffic behavior view | **traffic behavior** *behavior-name* | Required |
| Configure traffic mirroring action in the traffic behavior | **mirror-to** { **cpu** \| **interface** *interface-type interface-number* } | Required |

# Displaying and Maintaining Traffic Mirroring

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration information about the user-defined traffic behavior | **display traffic behavior user-defined** *behavior-name* | Available in any view |
| Display the configuration information about the user-defined policy | **display qos policy user-defined** *policy-name* | |

# Traffic Mirroring Configuration Example

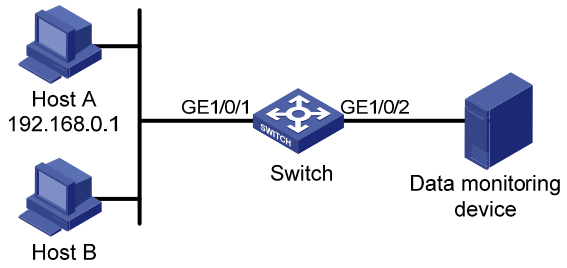
## Network Requirements

The user's network is as described below:

- Host A (with the IP address 192.168.0.1) and Host B are connected to GigabitEthernet1/0/1 of the switch.
- The data monitoring device is connected to GigabitEthernet1/0/2 of the switch.

It is required to monitor and analyze packets sent by Host A on the data monitoring device.

**Figure 6-1** Network diagram for configuring traffic mirroring to a port




## Configuration Procedure

Configure Switch:

# Enter system view.

```
<Sysname> system-view
```

# Configure basic IPv4 ACL 2000 to match packets with the source IP address 192.168.0.1.

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.0.1 0
[Sysname-acl-basic-2000] quit
```

# Configure a traffic classification rule to use ACL 2000 for traffic classification.

```
[Sysname] traffic classifier 1
[Sysname-classifier-1] if-match acl 2000
[Sysname-classifier-1] quit
```

# Configure a traffic behavior and define the action of mirroring traffic to GigabitEthernet1/0/2 in the traffic behavior.

```
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface GigabitEthernet 1/0/2
```

```
[Sysname-behavior-1] quit
```

# Configure a QoS policy and associate traffic behavior 1 with classification rule 1.

```
[Sysname] qos policy 1
[Sysname-policy-1] classifier 1 behavior 1
[Sysname-policy-1] quit
```

# Apply the policy in the inbound direction of GigabitEthernet1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy 1 inbound
```

After the configurations, you can monitor all packets sent from Host A on the data monitoring device.

# Table of Contents

# 1 User Profile Configuration

When configuring user profile, go to these sections for information you are interested in:



## User Profile Overview

User profile provides a configuration template to save predefined configurations. Based on different application scenarios, you can configure different items for a user profile, such as Committed Access Rate (CAR), Quality of Service (QoS), and so on.

When accessing the device, users need to be authenticated. During the authentication process, the authentication server sends the user profile name to the device, which then enables the configurations in the user profile. After the users pass the authentication and access the device, the device will restrict the users' access based on these configurations. When the users log out, the device automatically disables the configurations in the user profile, and thus the restrictions on the users are removed. Therefore, user profile is applicable to restricting online users' access; if no users are online (no user access, no users pass the authentication, or users have logged out), user profile does not take effect as it is a predefined configuration.

With user profile, you can:

- Make use of system resources more granularly. For example, without user profile, you can apply a QoS policy based on interface, VLAN, globally and so on. This QoS policy is applicable to a group of users. With user profile, however, you can apply a QoS policy on a per-user basis.
- Restrict users' access to the system resources more flexibly. For example, without user profile, you can perform traffic policing based on CAR, ACL, or for all the traffic of the current interface; when the physical position of users changes (for example, the users access the network using another interface), you need to configure traffic policing on another interface. With user profile, however, you can perform traffic policing on a per-user basis. As long as users are online, the authentication server applies the corresponding user profile (with CAR configured) to the users; when the users are offline, the system automatically removes the corresponding configuration.

## User Profile Configuration

### User Profile Configuration Task List

| Task | Remarks |
|---|---|
| Creating a User Profile | Required |
| Applying a QoS Policy to User Profile | Required |
| Enabling a User Profile | Required |

## Creating a User Profile

### Configuration Prerequisites

Before creating a user profile, you need to configure authentication parameters. User profile supports 802.1X authentications. You need to perform the related configurations (for example, username, password, authentication scheme, domain and binding between a user profile and user) on the client, the device and authentication server.

### Creating a User Profile

Follow these steps to create a user profile:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a user profile, and enter the corresponding user profile view | Create a user profile, and enter user-profile DOT1X view | **user-profile** *profile-name* **dot1x** | Required<br>If the specified user profile already exists, you will directly enter the corresponding user profile view.<br>The configuration made in user profile view takes effect when the user profile is enabled and the corresponding users are online. |

**Note**

Refer to *802.1x Configuration* in the *Security Volume* for detailed information about 802.1x authentication.

## Applying a QoS Policy to User Profile

After a user profile is created, you need to configure detailed items in user profile view to implement restrictions on the online users. Currently supported configurations are as follows:

Follow these steps to apply a QoS policy to traffic of online users:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter user profile view | **user-profile** *profile-name* [ **dot1x** ] | Required<br>The configuration made in user profile view takes effect when the user-profile is active and the corresponding users are online. |
| Apply the QoS policy | **qos apply policy** *policy-name* { **inbound** \| **outbound** } | Required |

**Note**

- When a user profile is active, you cannot configure or remove the QoS policy applied to it.
- The QoS policies applied in user profile view support only the **remark**, **car**, and **filter** actions.
- Do not apply an empty QoS policy in user profile view, because even if you can do that, the user profile cannot be activated.

### Enabling a User Profile

A created user profile takes effect only after being enabled.

Follow these steps to enable a user profile:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable a user profile | **user-profile** *profile-name* **enable** | Required<br>A user profile is disabled by default. |

**Caution**

- Only an enabled user profile can be used by a user. You cannot modify or remove the configuration items in a user profile until the user profile is disabled.
- Disabling a user profile logs out the users using the user profile.

## Displaying and Maintaining User Profile

| To do… | Use the command… |
|---|---|
| Display information about all the created user profiles | **display user-profile** |

# Security Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The Security Volume is organized as follows:

| Features | Description |
|---|---|
| AAA | Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management. This document describes:<br>• Introduction to AAA, RADIUS and HWTACACS<br>• AAA configuration<br>• RADIUS configuration<br>• HWTACACS configuration |
| 802.1X | IEEE 802.1X (hereinafter simplified as 802.1X) is a port-based network access control protocol that is used as the standard for LAN user access authentication. This document describes:<br>• 802.1X overview<br>• 802.1X configuration<br>• 802.1X Guest-VLAN configuration |
| HABP | On an HABP-capable switch, HABP packets can bypass 802.1X authentication and MAC authentication, allowing communication among switches in a cluster. This document describes:<br>• Introduction to HABP<br>• HABP configuration |
| MAC Authentication | MAC authentication provides a way for authenticating users based on ports and MAC addresses; it requires no client software to be installed on the hosts. This document describes:<br>• RADIUS-Based MAC Authentication<br>• Local MAC Authentication |
| Portal | Portal authentication, as its name implies, helps control access to the Internet. This document describes:<br>• Portal overview<br>• Portal configuration |

| Features | Description |
| --- | --- |
| Port Security | Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1X authentication and MAC authentication. This document describes:<br>• Enabling Port Security<br>• Setting the Maximum Number of Secure MAC Addresses<br>• Setting the Port Security Mode<br>• Configuring Port Security Features<br>• Configuring Secure MAC Addresses<br>• Ignoring Authorization Information from the Server |
| IP Source Guard | By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. This document describes:<br>• Configuring a Static Binding Entry<br>• Configuring Dynamic Binding Function |
| SSH2.0 | SSH ensures secure login to a remote device in a non-secure network environment. By encryption and strong authentication, it protects the device against attacks. This document describes:<br>• Configuring Asymmetric Keys<br>• Configuring the Device as an SSH Server<br>• Configuring the Device as an SSH Client<br>• Configuring an SFTP Server<br>• Configuring an SFTP Client |
| PKI | The Public Key Infrastructure (PKI) is a hierarchical framework designed for providing information security through public key technologies and digital certificates and verifying the identities of the digital certificate owners. This document describes PKI related configuration. |
| SSL | Secure Sockets Layer (SSL) is a security protocol providing secure connection service for TCP-based application layer protocols, this document describes SSL related configuration. |
| Public Key Configuration | This document describes Public Key Configuration. |
| ACL | An ACL is used for identifying traffic based on a series of preset matching criteria. This document describes:<br>• ACL overview and ACL types<br>• ACL configuration |

# Table of Contents

# 1 AAA Configuration

When configuring AAA, go to these sections for information you are interested in:

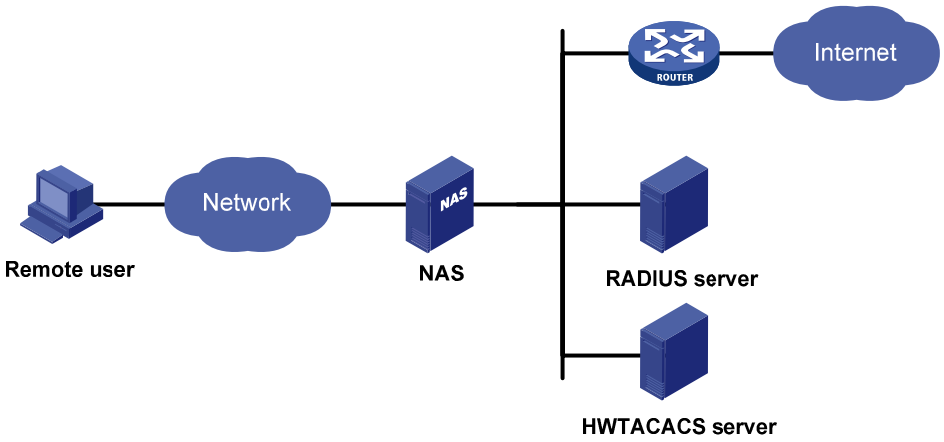


## Introduction to AAA

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for configuring these three security functions to implement network security management.

AAA usually uses a client/server model, where the client runs on the network access server (NAS) and the server maintains user information centrally. In an AAA network, a NAS is a server for users but a client for the AAA servers, as shown in Figure 1-1.

**Figure 1-1** AAA networking diagram




When a user tries to establish a connection to the NAS and to obtain the rights to access other networks or some network resources, the NAS authenticates the user or the corresponding connection. The NAS can transparently pass the user's AAA information to the server (RADIUS server or HWTACACS server). The RADIUS/HWTACACS protocol defines how a NAS and a server exchange user information between them.

In the AAA network shown in Figure 1-1, there is a RADIUS server and a HWTACACS server. You can determine the authentication, authorization and accounting methods according to the actual

requirements. For example, you can use the HWTACACS server for authentication and authorization, and the RADIUS server for accounting.

The three security functions are described as follows:

- Authentication: Identifies remote users and judges whether a user is legal.
- Authorization: Grants different users different rights. For example, a user logging into the server can be granted the permission to access and print the files in the server.
- Accounting: Records all network service usage information of users, including the service type, start and end time, and traffic. In this way, accounting can be used for not only charging, but also network security surveillance.

You can use AAA to provide only one or two security functions, if desired. For example, if your company only wants employees to be authenticated before they access specific resources, you only need to configure an authentication server. If network usage information is expected to be recorded, you also need to configure an accounting server.

As described above, AAA provides a uniform framework to implement network security management. It is a security mechanism that enables authenticated and authorized entities to access specific resources and records operations of the entities. The AAA framework thus allows for excellent scalability and centralized user information management.

AAA can be implemented through multiple protocols. Currently, the device supports using RADIUS, HWTACACS for AAA, and RADIUS is often used in practice.

# Introduction to RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol in a client/server model. RADIUS can protect networks against unauthorized access and is often used in network environments where both high security and remote user access are required. Based on UDP, RADIUS uses UDP port 1812 for authentication and 1813 for accounting. RADIUS defines the RADIUS packet format and message transfer mechanism.

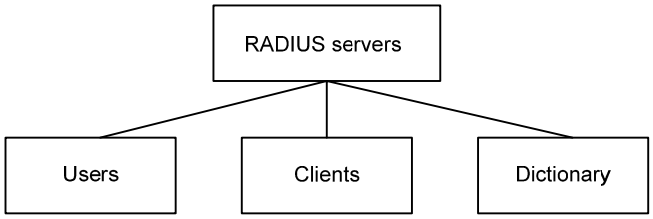
RADIUS was originally designed for dial-in user access. With the diversification of access methods, RADIUS has been extended to support more access methods, for example, Ethernet access and ADSL access. It uses authentication and authorization in providing access services and uses accounting to collect and record usage information of network resources.

## Client/Server Model

- Client: The RADIUS client runs on the NASs located throughout the network. It passes user information to designated RADIUS servers and acts on the responses (for example, rejects or accepts user access requests).
- Server: The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access. It listens to connection requests, authenticates users, and returns the processing results (for example, rejecting or accepting the user access request) to the clients.

In general, the RADIUS server maintains three databases, namely, Users, Clients, and Dictionary, as shown in Figure 1-2:

**Figure 1-2** RADIUS server components




- Users: Stores user information such as the usernames, passwords, applied protocols, and IP addresses.
- Clients: Stores information about RADIUS clients, such as the shared keys and IP addresses.
- Dictionary: Stores information about the meanings of RADIUS protocol attributes and their values.

## Security and Authentication Mechanisms

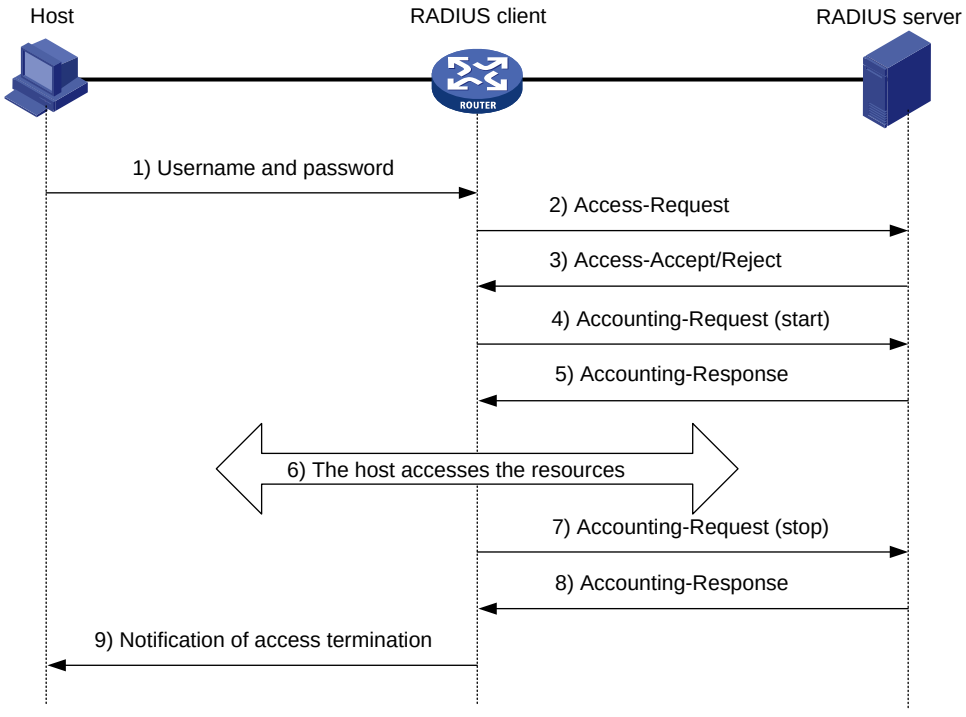
Information exchanged between a RADIUS client and the RADIUS server is authenticated with a shared key, which is never transmitted over the network. This enhances the information exchange security. In addition, to prevent user passwords from being intercepted in non-secure networks, RADIUS encrypts passwords before transmitting them.

A RADIUS server supports multiple user authentication methods, for example, the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Moreover, a RADIUS server can act as the client of another AAA server to provide authentication proxy services.

## Basic Message Exchange Process of RADIUS

Figure 1-3 illustrates the interaction of the host, the RADIUS client, and the RADIUS server.

**Figure 1-3** Basic message exchange process of RADIUS



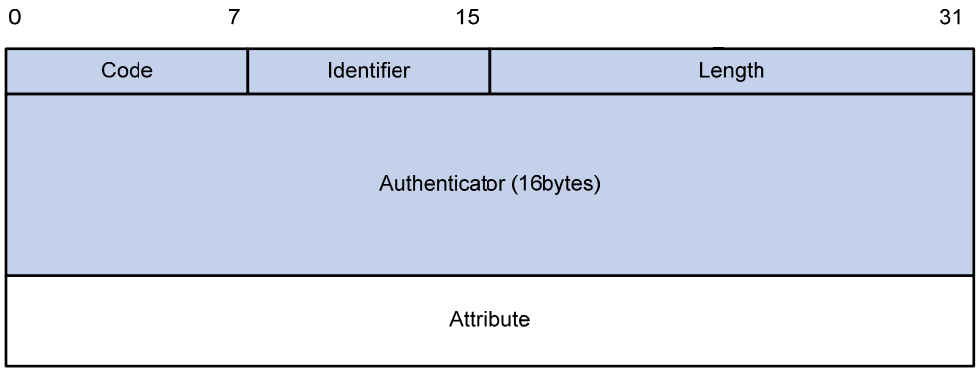

The following is how RADIUS operates:

1) The host initiates a connection request carrying the username and password to the RADIUS client.
2) Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.
3) The RADIUS server authenticates the username and password. If the authentication succeeds, it sends back an Access-Accept message containing the user's authorization information. If the authentication fails, it returns an Access-Reject message.
4) The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.
5) The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.
6) The user accesses the network resources.
7) The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.
8) The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.
9) The user stops access to network resources.

## RADIUS Packet Format

RADIUS uses UDP to transmit messages. It ensures the smooth message exchange between the RADIUS server and the client through a series of mechanisms, including the timer management mechanism, retransmission mechanism, and slave server mechanism. Figure 1-4 shows the RADIUS packet format.

**Figure 1-4** RADIUS packet format




Descriptions of the fields are as follows:

1) The Code field (1-byte long) is for indicating the type of the RADIUS packet. Table 1-1 gives the possible values and their meanings.

**Table 1-1** Main values of the Code field

| Code | Packet type | Description |
|---|---|---|
| 1 | Access-Request | From the client to the server. A packet of this type carries user information for the server to authenticate the user. It must contain the User-Name attribute and can optionally contain the attributes of NAS-IP-Address, User-Password, and NAS-Port. |

| Code | Packet type | Description |
|---|---|---|
| 2 | Access-Accept | From the server to the client. If all the attribute values carried in the Access-Request are acceptable, that is, the authentication succeeds, the server sends an Access-Accept response. |
| 3 | Access-Reject | From the server to the client. If any attribute value carried in the Access-Request is unacceptable, the server rejects the user and sends an Access-Reject response. |
| 4 | Accounting-Request | From the client to the server. A packet of this type carries user information for the server to start/stop accounting for the user. It contains the Acct-Status-Type attribute, which indicates whether the server is requested to start the accounting or to end the accounting. |
| 5 | Accounting-Response | From the server to the client. The server sends to the client a packet of this type to notify that it has received the Accounting-Request and has correctly started recording the accounting information. |

2) The Identifier field (1-byte long) is for matching request packets and response packets and detecting retransmitted request packets. The request and response packets of the same type have the same identifier.
3) The Length field (2-byte long) indicates the length of the entire packet, including the Code, Identifier, Length, Authenticator, and Attribute fields. The value of the field is in the range 20 to 4096. Bytes beyond the length are considered the padding and are neglected upon reception. If the length of a received packet is less than that indicated by the Length field, the packet is dropped.
4) The Authenticator field (16-byte long) is used to authenticate replies from the RADIUS server, and is also used in the password hiding algorithm. There are two kinds of authenticators: request authenticator and response authenticator.
5) The Attribute field, with a variable length, carries the specific authentication, authorization, and accounting information for defining configuration details of the request or response. This field is represented in triplets of Type, Length, and Value.

- Type: One byte, in the range 1 to 255. It indicates the type of the attribute. Commonly used attributes for RADIUS authentication, authorization and accounting are listed in Table 1-2.
- Length: One byte for indicating the length of the attribute in bytes, including the Type, Length, and Value fields.
- Value: Value of the attribute, up to 253 bytes. Its format and content depend on the Type and Length fields.

**Table 1-2** RADIUS attributes

| No. | Attribute | No. | Attribute |
|---|---|---|---|
| 1 | User-Name | 45 | Acct-Authentic |
| 2 | User-Password | 46 | Acct-Session-Time |
| 3 | CHAP-Password | 47 | Acct-Input-Packets |
| 4 | NAS-IP-Address | 48 | Acct-Output-Packets |
| 5 | NAS-Port | 49 | Acct-Terminate-Cause |

| No. | Attribute | No. | Attribute |
|---|---|---|---|
| 6 | Service-Type | 50 | Acct-Multi-Session-Id |
| 7 | Framed-Protocol | 51 | Acct-Link-Count |
| 8 | Framed-IP-Address | 52 | Acct-Input-Gigawords |
| 9 | Framed-IP-Netmask | 53 | Acct-Output-Gigawords |
| 10 | Framed-Routing | 54 | (unassigned) |
| 11 | Filter-ID | 55 | Event-Timestamp |
| 12 | Framed-MTU | 56-59 | (unassigned) |
| 13 | Framed-Compression | 60 | CHAP-Challenge |
| 14 | Login-IP-Host | 61 | NAS-Port-Type |
| 15 | Login-Service | 62 | Port-Limit |
| 16 | Login-TCP-Port | 63 | Login-LAT-Port |
| 17 | (unassigned) | 64 | Tunnel-Type |
| 18 | Reply_Message | 65 | Tunnel-Medium-Type |
| 19 | Callback-Number | 66 | Tunnel-Client-Endpoint |
| 20 | Callback-ID | 67 | Tunnel-Server-Endpoint |
| 21 | (unassigned) | 68 | Acct-Tunnel-Connection |
| 22 | Framed-Route | 69 | Tunnel-Password |
| 23 | Framed-IPX-Network | 70 | ARAP-Password |
| 24 | State | 71 | ARAP-Features |
| 25 | Class | 72 | ARAP-Zone-Access |
| 26 | Vendor-Specific | 73 | ARAP-Security |
| 27 | Session-Timeout | 74 | ARAP-Security-Data |
| 28 | Idle-Timeout | 75 | Password-Retry |
| 29 | Termination-Action | 76 | Prompt |
| 30 | Called-Station-Id | 77 | Connect-Info |
| 31 | Calling-Station-Id | 78 | Configuration-Token |
| 32 | NAS-Identifier | 79 | EAP-Message |
| 33 | Proxy-State | 80 | Message-Authenticator |
| 34 | Login-LAT-Service | 81 | Tunnel-Private-Group-id |
| 35 | Login-LAT-Node | 82 | Tunnel-Assignment-id |
| 36 | Login-LAT-Group | 83 | Tunnel-Preference |
| 37 | Framed-AppleTalk-Link | 84 | ARAP-Challenge-Response |
| 38 | Framed-AppleTalk-Network | 85 | Acct-Interim-Interval |
| 39 | Framed-AppleTalk-Zone | 86 | Acct-Tunnel-Packets-Lost |
| 40 | Acct-Status-Type | 87 | NAS-Port-Id |
| 41 | Acct-Delay-Time | 88 | Framed-Pool |

| No. | Attribute | No. | Attribute |
|---|---|---|---|
| 42 | Acct-Input-Octets | 89 | (unassigned) |
| 43 | Acct-Output-Octets | 90 | Tunnel-Client-Auth-id |
| 44 | Acct-Session-Id | 91 | Tunnel-Server-Auth-id |

**Note**

The attribute types listed in Table 1-2 are defined by RFC 2865, RFC 2866, RFC 2867, and RFC 2568.

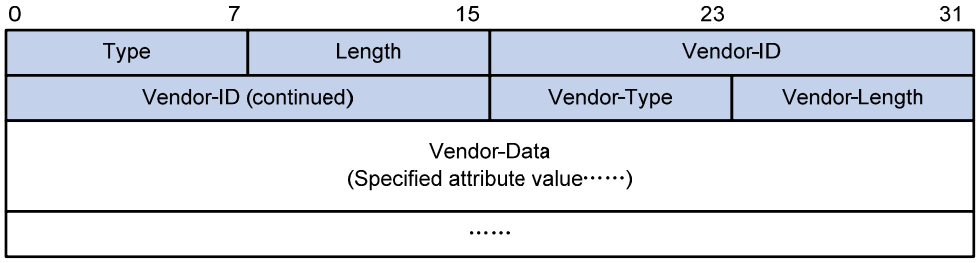
### Extended RADIUS Attributes

The RADIUS protocol features excellent extensibility. Attribute 26 (Vender-Specific) defined by RFC 2865 allows a vender to define extended attributes to implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple type-length-value (TLV) sub-attributes in RADIUS packets for extension in applications. As shown in Figure 1-5, a sub-attribute that can be encapsulated in Attribute 26 consists of the following four parts:

- Vendor-ID (four bytes): Indicates the ID of the vendor. Its most significant byte is 0 and the other three bytes contain a code complying with RFC 1700.
- Vendor-Type: Indicates the type of the sub-attribute.
- Vendor-Length: Indicates the length of the sub-attribute.
- Vendor-Data: Indicates the contents of the sub-attribute.

**Figure 1-5** Segment of a RADIUS packet containing an extended attribute




## Introduction to HWTACACS

HW Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to RADIUS, it uses a client/server model for information exchange between NAS and HWTACACS server.

HWTACACS is mainly used to provide AAA services for terminal users. In a typical HWTACACS application, a terminal user needs to log into the device for operations, and HWTACACS authenticates, authorizes and keeps accounting for the user. Working as the HWTACACS client, the device sends the username and password to the HWTACACS sever for authentication. After passing authentication and being authorized, the user can log into the device to perform operations.

## Differences Between HWTACACS and RADIUS

HWTACACS and RADIUS have many common features, like implementing AAA, using a client/server model, using shared keys for user information security and having good flexibility and extensibility. Meanwhile, they also have differences, as listed in Table 1-3.

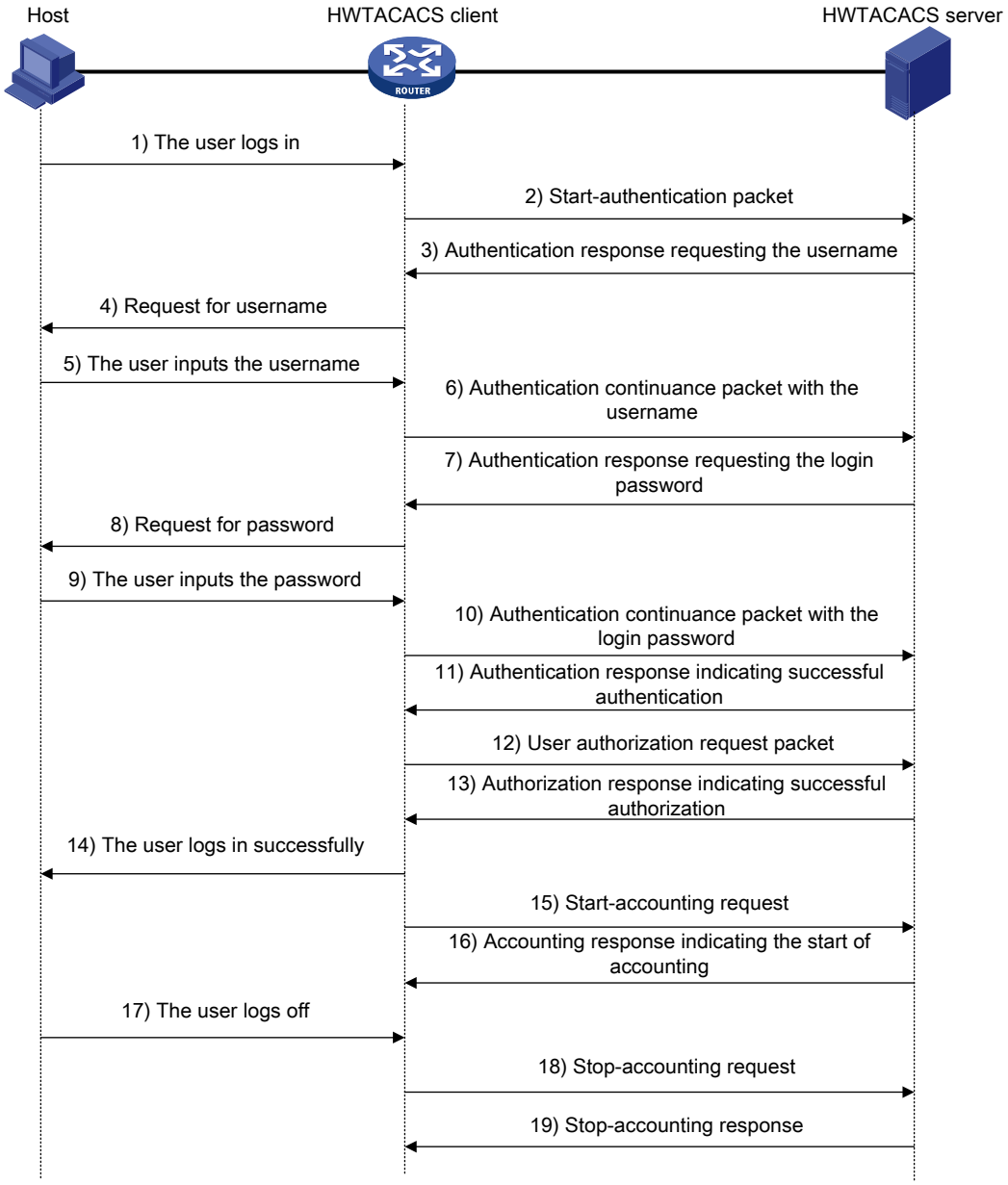
**Table 1-3** Primary differences between HWTACACS and RADIUS

| HWTACACS | RADIUS |
|---|---|
| Uses TCP, providing more reliable network transmission. | Uses UDP, providing higher transport efficiency. |
| Encrypts the entire packet except for the HWTACACS header. | Encrypts only the user password field in an authentication packet. |
| Protocol packets are complicated and authorization is independent of authentication. Authentication and authorization can be deployed on different HWTACACS servers. | Protocol packets are simple and authorization is combined with authentication. |
| Supports authorized use of configuration commands. For example, an authenticated login user can be authorized to configure the device. | Does not support authorized use of configuration commands. |

## Basic Message Exchange Process of HWTACACS

The following takes a Telnet user as an example to describe how HWTACACS performs user authentication, authorization, and accounting. Figure 1-6 illustrates the basic message exchange process of HWTACACS.

**Figure 1-6** Basic message exchange process of HWTACACS for a Telnet user




1) A Telnet user sends an access request to the NAS.
2) Upon receiving the request, the HWTACACS client sends a start-authentication packet to the HWTACACS server.
3) The HWTACACS server sends back an authentication response requesting the username.
4) Upon receiving the response, the HWTACACS client asks the user for the username.
5) The user inputs the username.
6) After receiving the username from the user, the HWTACACS client sends to the server a continue-authentication packet carrying the username.
7) The HWTACACS server sends back an authentication response, requesting the login password.
8) Upon receipt of the response, the HWTACACS client asks the user for the login password.
9) The user inputs the password.
10) After receiving the login password, the HWTACACS client sends to the HWTACACS server a continue-authentication packet carrying the login password.
11) The HWTACACS server sends back an authentication response indicating that the user has passed authentication.

12) The HWTACACS client sends the user authorization request packet to the HWTACACS server.
13) The HWTACACS server sends back the authorization response, indicating that the user is authorized now.
14) Knowing that the user is now authorized, the HWTACACS client pushes the configuration interface of the NAS to the user.
15) The HWTACACS client sends a start-accounting request to the HWTACACS server.
16) The HWTACACS server sends back an accounting response, indicating that it has received the start-accounting request.
17) The user logs off.
18) The HWTACACS client sends a stop-accounting request to the HWTACACS server.
19) The HWTACACS server sends back a stop-accounting response, indicating that the stop-accounting request has been received.

## Protocols and Standards

The protocols and standards related to AAA, RADIUS, HWTACACS include:

- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support
- RFC 2869: RADIUS Extensions
- RFC 1492: An Access Control Protocol, Sometimes Called TACACS

## AAA Configuration Task List

The basic procedure to configure AAA is as follows:

1) Configure the required AAA schemes.
- Local authentication: Configure local users and related attributes, including usernames and passwords of the users to be authenticated.
- Remote authentication: Configure the required RADIUS and/or HWTACACS schemes, and configure user attributes on the servers accordingly.

2) Configure the AAA methods: Reference the configured AAA schemes in the users' ISP domains.
- Authentication method: No authentication (**none**), local authentication (**local**), or remote authentication (**scheme**)
- Authorization method: No authorization (**none**) , local authorization (**local**), or remote authorization (**scheme**)
- Accounting method: No accounting (**none**), local accounting (**local**), or remote accounting (**scheme**)

---

 **Note**

For login users, it is necessary to configure the authentication mode for logging into the user interface as **scheme**. For detailed information, refer to *Login Configuration* of the *System Volume*.

---

## AAA Configuration Task List

| Task | Remarks |
|---|---|
| Creating an ISP Domain | Required |
| Configuring ISP Domain Attributes | Optional |
| Configuring AAA Authentication Methods for an ISP Domain | Required<br>For local authentication, refer to Configuring Local User Attributes.<br>For RADIUS authentication, refer to Configuring RADIUS.<br>For HWTACACS authentication, refer to Configuring HWTACACS. |
| Configuring AAA Authorization Methods for an ISP Domain | Optional |
| Configuring AAA Accounting Methods for an ISP Domain | Optional |
| Configuring Local User Attributes | Optional |
| Configuring User Group Attributes | Optional |
| Tearing down User Connections Forcibly | Optional |
| Displaying and Maintaining AAA | Optional |

## RADIUS Configuration Task List

| Task | Remarks |
|---|---|
| Creating a RADIUS Scheme | Required |
| Specifying the RADIUS Authentication/Authorization Servers | Required |
| Specifying the RADIUS Accounting Servers and Relevant Parameters | Optional |
| Setting the Shared Key for RADIUS Packets | Required |
| Setting the Upper Limit of RADIUS Request Retransmission Attempts | Optional |
| Setting the Supported RADIUS Server Type | Optional |
| Setting the Status of RADIUS Servers | Optional |
| Configuring Attributes Related to Data to Be Sent to the RADIUS Server | Optional |
| Setting Timers Regarding RADIUS Servers | Optional |
| Specifying Security Policy Servers | Optional |
| Enabling the Listening Port of the RADIUS Client | Optional |
| Displaying and Maintaining RADIUS | Optional |

### HWTACACS Configuration Task List

| Task | Remarks |
|---|---|
| Creating a HWTACACS scheme | Required |
| Specifying the HWTACACS Authentication Servers | Required |
| Specifying the HWTACACS Authorization Servers | Optional |
| Specifying the HWTACACS Accounting Servers | Optional |
| Setting the Shared Key for HWTACACS Packets | Required |
| Configuring Attributes Related to the Data Sent to HWTACACS Server | Optional |
| Setting Timers Regarding HWTACACS Servers | Optional |
| Displaying and Maintaining HWTACACS | Optional |

# Configuring AAA

By configuring AAA, you can provide network access service for legal users, protect the networking devices, and avoid unauthorized access and repudiation. In addition, you can configure ISP domains to perform AAA on accessing users.

In AAA, users are divided into LAN users (such as 802.1X users and MAC authentication users), login users (such as SSH, Telnet, FTP, and terminal access users), portal users and command line users (that is, command line authentication users). Except for command line users, you can configure separate authentication/authorization/accounting policies for all the other types of users. Command line users can be configured with authorization policy independently.

## Configuration Prerequisites

For remote authentication, authorization, or accounting, you must create the RADIUS or HWTACACS scheme first. For RADIUS scheme configuration, refer to Configuring RADIUS. For HWTACACS scheme configuration, refer to Configuring HWTACACS.

## Creating an ISP Domain

An Internet service provider (ISP) domain represents a group of users belonging to it. For a username in the *userid@isp-name* format, the access device considers the *userid* part the username for authentication and the *isp-name* part the domain name.

In a networking scenario with multiple ISPs, an access device may connect users of different ISPs. As users of different ISPs may have different user attributes (such as username and password structure, service type, and rights), you need to configure ISP domains to distinguish the users. In addition, you need to configure different attribute sets including AAA methods for the ISP domains.

For the NAS, each user belongs to an ISP domain. Up to 16 ISP domains can be configured on a NAS. If a user does not provide the ISP domain name, the system considers that the user belongs to the default ISP domain.

Follow these steps to create an ISP domain:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ISP domain and enter ISP domain view | **domain** *isp-name* | Required |
| Return to system view | **quit** | — |
| Specify the default ISP domain | **domain default enable** *isp-name* | Optional<br>By default, the system has a default ISP domain named **system**. |

**Note**

- You cannot delete the default ISP domain unless you change it to a non-default ISP domain (with the **domain default disable** command) first.
- If a user enters a username without an ISP domain name, the device uses the authentication method configured for the default ISP domain to authenticate the user.

## Configuring ISP Domain Attributes

Follow these steps to configure ISP domain attributes:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ISP domain and enter ISP domain view | **domain** *isp-name* | Required |
| Place the ISP domain to the state of active or blocked | **state** { **active** \| **block** } | Optional<br>When created, an ISP domain is in the active state by default, and users in the domain can request network services. |
| Specify the maximum number of active users in the ISP domain | **access-limit enable** *max-user-number* | Optional<br>No limit by default |
| Configure the idle cut function | **idle-cut enable** *minute* | Optional<br>Disabled by default<br>Currently, this command is effective only for LAN users. |
| Configure the self-service server localization function | **self-service-url enable** *url-string* | Optional<br>Disabled by default |

**Note**

A self-service RADIUS server, for example, comprehensive access management system (CAMS/iMC), is required for the self-service server localization function to work. With the self-service function, a user can manage and control his or her accounting information or card number. A server with self-service software is a self-service server.

## Configuring AAA Authentication Methods for an ISP Domain

In AAA, authentication, authorization, and accounting are separate processes. Authentication refers to the interactive authentication process of username/password/user information during access or service request. The authentication process neither sends authorization information to a supplicant nor triggers any accounting.

AAA supports the following authentication methods:

- No authentication: All users are trusted and no authentication is performed. Generally, this method is not recommended.
- Local authentication: Authentication is performed by the NAS, which is configured with the user information, including the usernames, passwords, and attributes. Local authentication features high speed and low cost, but the amount of information that can be stored is limited by the hardware.
- Remote authentication: The access device cooperates with a RADIUS or HWTACACS server to authenticate users. As for RADIUS, the device can use the standard RADIUS protocol or extended RADIUS protocol in collaboration with systems like CAMS/iMC to implement user authentication. Remote authentication features centralized information management, high capacity, high reliability, and support for centralized authentication for multiple devices. You can configure local authentication as the backup method in case the remote server is not available.

You can configure AAA authentication to work alone without authorization and accounting. By default, an ISP domain uses the local authentication method.

Before configuring authentication methods, complete these three tasks:

- For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme to be referenced first. The local and none authentication methods do not require any scheme.
- Determine the access mode or service type to be configured. With AAA, you can configure an authentication method specifically for each access mode and service type, limiting the authentication protocols that can be used for access.
- Determine whether to configure an authentication method for all access modes or service types.

Follow these steps to configure AAA authentication methods for an ISP domain:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ISP domain and enter ISP domain view | **domain** *isp-name* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify the default authentication method for all types of users | **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>**local** by default |
| Specify the authentication method for LAN users | **authentication lan-access** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authentication method is used by default. |
| Specify the authentication method for login users | **authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authentication method is used by default. |
| Specify the authentication method for portal users | **authentication portal** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authentication method is used by default. |

**Note**

- The authentication method specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.
- With an authentication method that references a RADIUS scheme, AAA accepts only the authentication result from the RADIUS server. The Access-Accept message from the RADIUS server does include the authorization information, but the authentication process ignores the information.
- With the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** keyword and argument combination configured, local authentication is the backup method and is used only when the remote server is not available.
- If the primary authentication method is **local** or **none**, the system performs local authentication or does not perform any authentication, and will not use any RADIUS or HWTACACS authentication scheme.

## Configuring AAA Authorization Methods for an ISP Domain

In AAA, authorization is a separate process at the same level as authentication and accounting. Its responsibility is to send authorization requests to the specified authorization server and to send authorization information to users. Authorization method configuration is optional in AAA configuration.

AAA supports the following authorization methods:

- No authorization: Every user is trusted and has the corresponding default rights of the system.
- Local authorization: Users are authorized by the access device according to the attributes configured for them.
- Remote authorization: The access device cooperates with a RADIUS or HWTACACS server to authorize users. RADIUS authorization is bound with RADIUS authentication. RADIUS authorization can work only after RADIUS authentication is successful, and the authorization

information is carried in the Access-Accept message. HWTACACS authorization is separate from HWTACACS authentication, and the authorization information is carried in the authorization response after successful authentication. You can configure local authorization or no authorization as the backup method in case the remote server is not available.

By default, an ISP domain uses the local authorization method. If the no authorization method (**none**) is configured, the users are not required to be authorized, in which case an authenticated user has the default right. The default right is visiting (the lowest one) for EXEC users (that is, console users who use the console, AUX port, or Telnet to connect to the device, such as Telnet or SSH users. Each connection of these types is called an EXEC user). The default right for FTP users is to use the root directory of the device.

Before configuring authorization methods, complete these three tasks:

1) For HWTACACS authorization, configure the HWTACACS scheme to be referenced first. For RADIUS authorization, the RADIUS authorization scheme must be the same as the RADIUS authentication scheme; otherwise, it does not take effect.
2) Determine the access mode or service type to be configured. With AAA, you can configure an authorization scheme specifically for each access mode and service type, limiting the authorization protocols that can be used for access.
3) Determine whether to configure an authorization method for all access modes or service types.

Follow these steps to configure AAA authorization methods for an ISP domain:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ISP domain and enter ISP domain view | **domain** *isp*-name | Required |
| Specify the default authorization method for all types of users | **authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>**local** by default |
| Specify the authorization method for command line users | **authorization command** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** \| **none** ] \| **local** \| **none** } | Optional<br>The default authorization method is used by default. |
| Specify the authorization method for LAN users | **authorization lan-access** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authorization method is used by default. |
| Specify the authorization method for login users | **authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authorization method is used by default. |
| Specify the authorization method for portal users | **authorization portal** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default authorization method is used by default. |

**Note**

- The authorization method specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.
- With the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** | **none** ] keyword and argument combination configured, local authorization or no authorization is the backup method and is used only when the remote server is not available.
- If the primary authorization method is **local** or **none**, the system performs local authorization or does not perform any authorization; it will never use the RADIUS or HWTACACS authorization scheme.
- The authorization information of the RADIUS server is sent to the RADIUS client along with the authentication response message; therefore, you cannot specify a separate RADIUS authorization server. If you use RADIUS for authorization and authentication, you must use the same scheme setting for authorization and authentication; otherwise, the system will prompt you with an error message.

## Configuring AAA Accounting Methods for an ISP Domain

In AAA, accounting is a separate process at the same level as authentication and authorization. Its responsibility is to send accounting start/update/end requests to the specified accounting server. Accounting is not required, and therefore accounting method configuration is optional.

AAA supports the following accounting methods:

- No accounting: The system does not perform accounting for the users.
- Local accounting: Local accounting is implemented on the access device. It is for collecting statistics on the number of users and controlling the number of local user connections; it does not provide statistics for user charge.
- Remote accounting: The access device cooperates with a RADIUS server or HWTACACS server for accounting of users. You can configure local accounting as the backup method in case the remote server is not available.

By default, an ISP domain uses the local accounting method.

Before configuring accounting methods, complete these three tasks:

1) For RADIUS or HWTACACS accounting, configure the RADIUS or HWTACACS scheme to be referenced first. The local and none authentication methods do not require any scheme.
2) Determine the access mode or service type to be configured. With AAA, you can configure an accounting method specifically for each access mode and service type, limiting the accounting protocols that can be used for access.
3) Determine whether to configure an accounting method for all access modes or service types.

Follow these steps to configure AAA accounting methods for an ISP domain:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ISP domain and enter ISP domain view | **domain** *isp-name* | Required |
| Enable the accounting optional feature | **accounting optional** | Optional<br>Disabled by default |
| Specify the default accounting method for all types of users | **accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>**local** by default |
| Specify the accounting method for LAN users | **accounting lan-access** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default accounting method is used by default. |
| Specify the accounting method for login users | **accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default accounting method is used by default. |
| Specify the accounting method for portal users | **accounting portal** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | Optional<br>The default accounting method is used by default. |

**Note**

- With the **accounting optional** command configured, a user to be disconnected can still use the network resources even when there is no available accounting server or communication with the current accounting server fails.
- The local accounting is not used for accounting implementation, but together with the **attribute access-limit** command for limiting the number of local user connections. However, with the **accounting optional** command configured, the limit on the number of local user connections is not effective.
- The accounting method specified with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.
- With the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** keyword and argument combination configured, local accounting is the backup method and is used only when the remote server is not available.
- If the primary accounting method is **local** or **none**, the system performs local accounting or does not perform any accounting, and will not use the RADIUS or HWTACACS accounting scheme.
- In login access mode, accounting is not supported for FTP services.

## Configuring Local User Attributes

For local authentication, you need to create local users and configure user attributes on the device as needed.

A local user represents a set of user attributes configured on a device, and such a user set is uniquely identified by the username. For a user requesting network service to pass local authentication, you must add an entry as required in the local user database of the device.

Each local user belongs to a local user group and bears all attributes of the group, such as the password control attributes and authorization attributes. For details about local user group, refer to Configuring User Group Attributes.

When configuring local users and local user groups, pay attention to the effective ranges and priority relationship of user group attributes and user attributes:

- Authorization attributes

You can configure an authorization attribute in user group view or local user view, making the attribute effective on all local users of the group or only the local user. An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.

Follow these steps to configure the attributes for a local user:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the password display mode for all local users | **local-user password-display-mode** { **auto** \| **cipher-force** } | Optional<br>**auto** by default, indicating to display the password of a local user in the way indicated by the **password** command. |
| Add a local user and enter local user view | **local-user** *user-name* | Required<br>No local user exists by default. |
| Configure a password for the local user | **password** { **cipher** \| **simple** } *password* | Optional |
| Place the local user to the state of active or blocked | **state** { **active** \| **block** } | Optional<br>When created, a local user is in the state of active by default, and the user can request network services. |
| Set the maximum number of user connections using the local user account | **access-limit** *max-user-number* | Optional<br>By default, there is no limit on the maximum number of user connections using the same local user account. |
| Specify the service types for the local user | **service-type** { **ftp** \| **lan-access** \| { **ssh** \| **telnet** \| **terminal** } * \| **portal** } | Optional<br>By default, no service is authorized to a user. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the binding attributes for the local user | **bind-attribute** { **call-number** *call-number* [ : *subcall-number* ] \| **ip** *ip-address* \| **location port** *slot-number subslot-number port-number* \| **mac** *mac-address* \| **vlan** *vlan-id* } * | Optional<br>By default, no binding attribute is configured for a local user. |
| Configure the authorization attributes for the local user | **authorization-attribute** { **acl** *acl-number* \| **callback-number** *callback-number* \| **idle-cut** *minute* \| **level** *level* \| **user-profile** *profile-name* \| **vlan** *vlan-id* \| **work-directory** *directory-name* } * | Optional<br>By default, no authorization attribute is configured for a local user. |
| Set the expiration time of the user | **expiration-date** *time* | Optional<br>Not set by default |
| Specify the user group for the local user | **group** *group-name* | Optional<br>By default, a local user belongs to default user group **system**. |

Note that:

- With the **local-user password-display-mode cipher-force** command configured, a local user password is always displayed in cipher text, regardless of the configuration of the **password** command. In this case, if you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.
- The **access-limit** command configured for a local user takes effect only when local accounting is used.
- Local authentication checks the service types of a local user. If the service types are not available, the user cannot pass authentication.
- In the authentication method that requires the username and password, including local authentication, RADIUS authentication and HWTACACS authentication, the commands that a login user can use after logging in depend on the level of the user. In other authentication methods, which commands are available depends on the level of the user interface. For an SSH user using public key authentication, the commands that can be used depend on the level configured on the user interface. For details regarding authentication method and commands accessible to user interface, refer to *Login Configuration* in the *System Volume.*
- Binding attributes are checked upon authentication of a local user. If the checking fails, the user fails the authentication. Therefore, be cautious when deciding which binding attributes should be configured for a local user.
- Every configurable authorization attribute has its definite application environments and purposes. Therefore, when configuring authorization attributes for a local user, consider what attributes are needed.

## Configuring User Group Attributes

For simplification of local user configuration and manageability of local users, the concept of user group is introduced. A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user

attributes for the local users in the group. Currently, you can configure password control attributes and authorization attributes for a user group.

By default, every newly added local user belongs to the user group of system and bears all attributes of the group. User group system is automatically created by the device.

Follow these steps to configure the attributes for a user group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a user group and enter user group view | **user-group** *group-name* | Required |
| Configure the authorization attributes for the user group | **authorization-attribute** { **acl** *acl-number* \| **callback-number** *callback-number* \| **idle-cut** *minute* \| **level** *level* \| **user-profile** *profile-name* \| **vlan** *vlan-id* \| **work-directory** *directory-name* } * | Optional<br>By default, no authorization attribute is configured for a user group. |

## Tearing down User Connections Forcibly

Follow these steps to tear down user connections forcibly:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Tear down AAA user connections forcibly | **cut connection** { **all** \| **domain** *isp-name* \| **ucibindex** *ucib-index* \| **user-name** *user-name* } | Required<br>Applies to only LAN access and portal user connections at present |

## Displaying and Maintaining AAA

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration information of a specified ISP domain or all ISP domains | **display domain** [ *isp-name* ] | Available in any view |
| Display information about specified or all user connections | **display connection** [ **domain** *isp-name* \| **ucibindex** *ucib-index* \| **user-name** *user-name*] | Available in any view |
| Display information about specified or all local users | **display local-user** [ **idle-cut** { **disable** \| **enable** } \| **service-type** { **ftp** \| **lan-access** \| **portal** \| **ssh** \| **telnet** \| **terminal** } \| **state** { **active** \| **block** } \| **user-name** *user-name* \| **vlan** *vlan-id* ] | Available in any view |
| Display configuration information about a specified user group or all user groups | **display user-group** [ *group-name* ] | Available in any view |

# Configuring RADIUS

The RADIUS protocol is configured on a per scheme basis. After creating a RADIUS scheme, you need to configure the IP addresses and UDP ports of the RADIUS servers for the scheme. The servers include authentication/authorization servers and accounting servers, or primary servers and secondary servers. In other words, the attributes of a RADIUS scheme mainly include IP addresses of primary and secondary servers, shared key, and RADIUS server type.

Actually, the RADIUS protocol configurations only set the parameters necessary for the information interaction between a NAS and a RADIUS server. For these settings to take effect, you must reference the RADIUS scheme containing those settings in ISP domain view. For information about the commands for referencing a scheme, refer to Configuring AAA.

**Note**

When there are users online, you cannot modify RADIUS parameters other than the retransmission ones and the timers.

## Creating a RADIUS Scheme

Before performing other RADIUS configurations, follow these steps to create a RADIUS scheme and enter RADIUS scheme view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |

**Note**

A RADIUS scheme can be referenced by more than one ISP domain at the same time.

## Specifying the RADIUS Authentication/Authorization Servers

Follow these steps to specify the RADIUS authentication/authorization servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Specify the primary RADIUS authentication/authorization server | **primary authentication** *ip-address* [ *port-number* ] | Required<br>Configure at least one of the |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify the secondary RADIUS authentication/authorization server | **secondary authentication** *ip-address* [ *port-number* ] | commands<br>No authentication server by default |

**Note**

- It is recommended to specify only the primary RADIUS authentication/authorization server if backup is not required.
- If both the primary and secondary authentication/authorization servers are specified, the secondary one is used when the primary one is unreachable.
- In practice, you may specify two RADIUS servers as the primary and secondary authentication/authorization servers respectively. At one time, a server can be the primary authentication/authorization server for a scheme and the secondary authentication/authorization servers for another scheme.
- The IP addresses of the primary and secondary authentication/authorization servers for a scheme cannot be the same. Otherwise, the configuration fails.

## Specifying the RADIUS Accounting Servers and Relevant Parameters

Follow these steps to specify the RADIUS accounting servers and perform related configurations:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Specify the primary RADIUS accounting server | **primary accounting** *ip-address* [ *port-number* ] | Required<br>Configure at least one of the commands<br>No accounting server by default |
| Specify the secondary RADIUS accounting server | **secondary accounting** *ip-address* [ *port-number* ] | |
| Enable the device to buffer stop-accounting requests getting no responses | **stop-accounting-buffer enable** | Optional<br>Enabled by default |
| Set the maximum number of stop-accounting request transmission attempts | **retry stop-accounting** *retry-times* | Optional<br>500 by default |
| Set the maximum number of accounting request transmission attempts | **retry realtime-accounting** *retry-times* | Optional<br>5 by default |

**Note**

- It is recommended to specify only the primary RADIUS accounting server if backup is not required.
- If both the primary and secondary accounting servers are specified, the secondary one is used when the primary one is not reachable.
- In practice, you can specify two RADIUS servers as the primary and secondary accounting servers respectively, or specify one server to function as the primary accounting server in a scheme and the secondary accounting server in another scheme. Besides, because RADIUS uses different UDP ports to receive authentication/authorization and accounting packets, the port for authentication/authorization must be different from that for accounting.
- You can set the maximum number of stop-accounting request transmission buffer, allowing the device to buffer and resend a stop-accounting request until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the device discards the packet.
- You can set the maximum number of accounting request transmission attempts on the device, allowing the device to disconnect a user when the number of accounting request transmission attempts for the user reaches the limit but it still receives no response to the accounting request.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- Currently, RADIUS does not support keeping accounts on FTP users.

## Setting the Shared Key for RADIUS Packets

The RADIUS client and RADIUS server use the MD5 algorithm to encrypt packets exchanged between them and a shared key to verify the packets. Only when the same key is used can they properly receive the packets and make responses.

Follow these steps to set the shared key for RADIUS packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Set the shared key for RADIUS authentication/authorization or accounting packets | **key** { **accounting** \| **authentication** } *string* | Required<br>No key by default |

**Note**

The shared key configured on the device must be the same as that configured on the RADIUS server.

## Setting the Upper Limit of RADIUS Request Retransmission Attempts

Because RADIUS uses UDP packets to carry data, the communication process is not reliable. If a NAS receives no response from the RADIUS server before the response timeout timer expires, it is required

to retransmit the RADIUS request. If the number of transmission attempts exceeds the specified limit but it still receives no response, it considers that the authentication has failed.

Follow these steps to set the upper limit of RADIUS request retransmission attempts:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Set the number of retransmission attempts of RADIUS packets | **retry** *retry-times* | Optional<br>3 by default |

**Note**

- The maximum number of retransmission attempts of RADIUS packets multiplied by the RADIUS server response timeout period cannot be greater than 75.
- Refer to the **timer response-timeout** command in the command manual for configuring RADIUS server response timeout period.

## Setting the Supported RADIUS Server Type

Follow these steps to set the supported RADIUS server type:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Specify the RADIUS server type supported by the device | **server-type** { **extended** \| **standard** } | Optional<br>By default, the supported RADIUS server type is **standard**. |

**Note**

- If you change the type of RADIUS server, the data stream destined to the original RADIUS server will be restored to the default unit.
- When a third-party RADIUS is used, you can configure the RADIUS server to **standard** or **extended**. When CAMS/iMC server is used, you must configure the RADIUS server to **extended.**

## Setting the Status of RADIUS Servers

When a primary server fails, the device automatically tries to communicate with the secondary server.

When both the primary and secondary servers are available, the device sends request packets to the primary server.

Once the primary server fails, the primary server turns into the state of block, and the device turns to the secondary server. In this case:

- If the secondary server is available, the device triggers the primary server quiet timer. After the quiet timer times out, the status of the primary server is active again and the status of the secondary server remains the same.
- If the secondary server fails, the device restores the status of the primary server to active immediately.

If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. After accounting starts, the communication between the client and the secondary server remains unchanged.

Follow these steps to set the status of RADIUS servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Set the status of the primary RADIUS authentication/authorization server | **state primary authentication** { **active** \| **block** } | Optional<br>**active** for every server configured with IP address in the RADIUS scheme |
| Set the status of the primary RADIUS accounting server | **state primary accounting** { **active** \| **block** } | |
| Set the status of the secondary RADIUS authentication/authorization server | **state secondary authentication** { **active** \| **block** } | |
| Set the status of the secondary RADIUS accounting server | **state secondary accounting** { **active** \| **block** } | |

**Note**

- If both the primary server and the secondary server are in the blocked state, it is necessary to manually turn the secondary server to the active state so that the secondary server can perform authentication. If the secondary server is still in the blocked state, the primary/secondary switchover cannot take place.
- If one server is in the active state while the other is blocked, the primary/secondary switchover will not take place even if the active server is not reachable.
- The server status set by the **state** command cannot be saved in the configuration file and will be restored to **active** every time the server restarts.

## Configuring Attributes Related to Data to Be Sent to the RADIUS Server

Follow these steps to configure the attributes related to data to be sent to the RADIUS server:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable the RADIUS trap function | | **radius trap** { **accounting-server-down** \| **authentication-server-down** } | Optional<br>Disabled by default |
| Create a RADIUS scheme and enter RADIUS scheme view | | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Specify the format of the username to be sent to a RADIUS server | | **user-name-format** { **keep-original** \| **with-domain** \| **without-domain** } | Optional<br>By default, the ISP domain name is included in the username. |
| Specify the unit for data flows or packets to be sent to a RADIUS server | | **data-flow-format** { **data** { **byte** \| **giga-byte** \| **kilo-byte** \| **mega-byte** } \| **packet** { **giga-packet** \| **kilo-packet** \| **mega-packet** \| **one-packet** } }* | Optional<br>The defaults are as follows:<br>**byte** for data flows, and **one-packet** for data packets. |
| Set the source IP address of the device to send RADIUS packets | In RADIUS scheme view | **nas-ip** *ip-address* | Use either command<br>By default, the outbound port serves as the source IP address to send RADIUS packets |
| | In system view | **quit** | |
| | | **radius nas-ip** *ip-address* | |

**Note**

- Some earlier RADIUS servers cannot recognize usernames that contain an ISP domain name. In this case, the device must remove the domain name before sending a username including a domain name. You can configure the **user-name-format without-domain** command on the device for this purpose.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same userid as one.
- The unit of data flows sent to the RADIUS server must be consistent with the traffic statistics unit of the RADIUS server. Otherwise, accounting cannot be performed correctly.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view takes precedence over the **radius nas-ip** command.

## Setting Timers Regarding RADIUS Servers

When communicating with the RADIUS server, a device can enable the following three timers:

- RADIUS server response timeout (**response-timeout**): If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

- Primary server quiet timer (**timer quiet**): If the primary server is not reachable, its state changes to blocked, and the device will turn to the specified secondary server. If the secondary server is reachable, the device starts this timer and communicates with the secondary server. After this timer expires, the device turns the state of the primary server to active and tries to communicate with the primary server while keeping the state of the secondary server unchanged. If the primary server has come back into operation, the device interacts with the primary server and terminates its communication with the secondary server.
- Real-time accounting interval (**realtime-accounting**): This timer defines the interval for performing real-time accounting of users. After this timer is set, the switch will send accounting information of online users to the RADIUS server at the specified interval.

Follow these steps to set timers regarding RADIUS servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter RADIUS scheme view | **radius scheme** *radius-scheme-name* | Required<br>Not defined by default |
| Set the RADIUS server response timeout timer | **timer response-timeout** *seconds* | Optional<br>3 seconds by default |
| Set the quiet timer for the primary server | **timer quiet** *minutes* | Optional<br>5 minutes by default |
| Set the real-time accounting interval | **timer realtime-accounting** *minutes* | Optional<br>12 minutes by default |

**Note**

- The maximum number of retransmission attempts of RADIUS packets multiplied by the RADIUS server response timeout period cannot be greater than 75. This product is also the upper limit of the timeout time of different access modules.
- For an access module, the maximum number of retransmission attempts multiplied by the RADIUS server response timeout period must be smaller than the timeout time. Otherwise, stop-accounting messages cannot be buffered, and the primary/secondary server switchover cannot take place. For example, as the timeout time of voice access is 10 seconds, the product of the two parameters cannot exceed 10 seconds; as the timeout time of Telnet access is 30 seconds, the product of the two parameters cannot exceed 30 seconds. For detailed information about timeout time of a specific access module, refer to the corresponding part in the *Access Volume.*
- To configure the maximum number of retransmission attempts of RADIUS packets, refer to the command **retry** in the command manual.

## Specifying Security Policy Servers

The core of the EAD solution is integration and cooperation, and the security policy server system is the management and control center. As a collection of software, the security policy server system can run on Windows and Linux to provide functions such as user management, security policy management, security status assessment, security cooperation control, and security event audit.

Follow these steps to specify a security policy server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a RADIUS scheme and enter its view | **radius scheme** *radius-scheme-name* | Required<br>By default, no RADIUS scheme is present. |
| Specify a security policy server | **security-policy-server** *ip-address* | Optional<br>Not specified by default |

**Note**

- If more than one interface of the device is configured with user access authentication functions, the interfaces may use different security policy servers. You can specify up to eight security policy servers for a RADIUS scheme.
- If the RADIUS server and the security policy server reside on the same physical device, you do not need to configure the IP address of the security policy server.
- The specified security policy server must be a security policy server or RADIUS server that is correctly configured and working normally. Otherwise, the device will regard it as an illegal server.

## Enabling the Listening Port of the RADIUS Client

Follow these steps to enable the listening port of the RADIUS client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the listening port of the RADIUS client | **radius client enable** | Optional<br>Enabled by default |

## Displaying and Maintaining RADIUS

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration information of a specified RADIUS scheme or all RADIUS schemes | **display radius scheme** [ *radius-scheme-name* ] | Available in any view |
| Display statistics about RADIUS packets | **display radius statistics** | Available in any view |
| Display information about buffered stop-accounting requests that get no responses | **display stop-accounting-buffer** { **radius-scheme** *radius-server-name* \| **session-id** *session-id* \| **time-range** *start-time stop-time* \| **user-name** *user-name* } | Available in any view |
| Clear RADIUS statistics | **reset radius statistics** | Available in user view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear buffered stop-accounting requests that get no responses | **reset stop-accounting-buffer** { **radius-scheme** *radius-server-name* \| **session-id** *session-id* \| **time-range** *start-time stop-time* \| **user-name** *user-name* } | Available in user view |

# Configuring HWTACACS

**Note**

Different from RADIUS, except for deleting HWTACACS schemes and changing the IP addresses of the HWTACACS servers, you can make any changes to HWTACACS parameters, whether there are users online or not.

## Creating a HWTACACS scheme

The HWTACACS protocol is configured on a per scheme basis. Before performing other HWTACACS configurations, follow these steps to create a HWTACACS scheme and enter HWTACACS scheme view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |

**Note**

- Up to 16 HWTACACS schemes can be configured.
- A scheme can be deleted only when it is not referenced.

## Specifying the HWTACACS Authentication Servers

Follow these steps to specify the HWTACACS authentication servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify the primary HWTACACS authentication server | **primary authentication** *ip-address* [ *port-number* ] | Required<br>Configure at least one of the commands<br>No authentication server by default |
| Specify the secondary HWTACACS authentication server | **secondary authentication** *ip-address* [ *port-number* ] | |

**Note**

- It is recommended to specify only the primary HWTACACS authentication server if backup is not required.
- If both the primary and secondary authentication servers are specified, the secondary one is used when the primary one is not reachable.
- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

## Specifying the HWTACACS Authorization Servers

Follow these steps to specify the HWTACACS authorization servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |
| Specify the primary HWTACACS authorization server | **primary authorization** *ip-address* [ *port-number* ] | Required<br>Configure at least one of the commands<br>No authorization server by default |
| Specify the secondary HWTACACS authorization server | **secondary authorization** *ip-address* [ *port-number* ] | |

**Note**

- It is recommended to specify only the primary HWTACACS authorization server if backup is not required.
- If both the primary and secondary authorization servers are specified, the secondary one is used when the primary one is not reachable.
- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

## Specifying the HWTACACS Accounting Servers

Follow these steps to specify the HWTACACS accounting servers and perform related configurations:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |
| Specify the primary HWTACACS accounting server | **primary accounting** *ip-address* [ *port-number* ] | Required<br>Configure at least one of the commands<br>No accounting server by default |
| Specify the secondary HWTACACS accounting server | **secondary accounting** *ip-address* [ *port-number* ] | |
| Enable the device to buffer stop-accounting requests getting no responses | **stop-accounting-buffer enable** | Optional<br>Enabled by default |
| Set the maximum number of stop-accounting request transmission attempts | **retry stop-accounting** *retry-times* | Optional<br>100 by default |

**Note**

- It is recommended to specify only the primary HWTACACS accounting server if backup is not required.
- If both the primary and secondary accounting servers are specified, the secondary one is used when the primary one is not reachable.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.
- Currently, HWTACACS does not support keeping accounts on FTP users.

## Setting the Shared Key for HWTACACS Packets

When using a HWTACACS server as an AAA server, you can set a key to secure the communications between the device and the HWTACACS server.

The HWTACACS client and HWTACACS server use the MD5 algorithm to encrypt packets exchanged between them and a shared key to verify the packets. Only when the same key is used can they properly receive the packets and make responses.

Follow these steps to set the shared key for HWTACACS packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |
| Set the shared keys for HWTACACS authentication, authorization, and accounting packets | **key** { **accounting** \| **authentication** \| **authorization** } *string* | Required<br>No shared key exists by default. |

## Configuring Attributes Related to the Data Sent to HWTACACS Server

Follow these steps to configure the attributes related to the data sent to the HWTACACS server:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |
| Specify the format of the username to be sent to a HWTACACS server | | **user-name-format** { **keep-original** \| **with-domain** \| **without-domain** } | Optional<br>By default, the ISP domain name is included in the username. |
| Specify the unit for data flows or packets to be sent to a HWTACACS server | | **data-flow-format** { **data** { **byte** \| **giga-byte** \| **kilo-byte** \| **mega-byte** } \| **packet** { **giga-packet** \| **kilo-packet** \| **mega-packet** \| **one-packet** } }* | Optional<br>The defaults are as follows:<br>**byte** for data flows, and<br>**one-packet** for data packets. |
| Set the source IP address of the device to send HWTACACS packets | In HWTACACS scheme view | **nas-ip** *ip-address* | Use either command<br>By default, the outbound port serves as the source IP address to send HWTACACS packets. |
| | In system view | **quit** | |
| | | **hwtacacs nas-ip** *ip-address* | |

**Note**

- If a HWTACACS server does not support a username with the domain name, you can configure the device to remove the domain name before sending the username to the server.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

## Setting Timers Regarding HWTACACS Servers

Follow these steps to set timers regarding HWTACACS servers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a HWTACACS scheme and enter HWTACACS scheme view | **hwtacacs scheme** *hwtacacs-scheme-name* | Required<br>Not defined by default |
| Set the HWTACACS server response timeout timer | **timer response-timeout** *seconds* | Optional<br>5 seconds by default |
| Set the quiet timer for the primary server | **timer quiet** *minutes* | Optional<br>5 minutes by default |
| Set the real-time accounting interval | **timer realtime-accounting** *minutes* | Optional<br>12 minutes by default |

**Note**

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. Note that if the device does not receive any response to the information, it does not disconnect the online users forcibly
- The real-time accounting interval must be a multiple of 3.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance.

## Displaying and Maintaining HWTACACS

| To do… | Use the command… | Remarks |
|---|---|---|
| Display configuration information or statistics of the specified or all HWTACACS schemes | **display hwtacacs** [ *hwtacacs-server-name* [ **statistics** ] ] | Available in any view |
| Display information about buffered stop-accounting requests that get no responses | **display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name* | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear HWTACACS statistics | **reset hwtacacs statistics** { **accounting** \| **all** \| **authentication** \| **authorization** } | Available in user view |
| Clear buffered stop-accounting requests that get no responses | **reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name* | Available in user view |

# AAA Configuration Examples

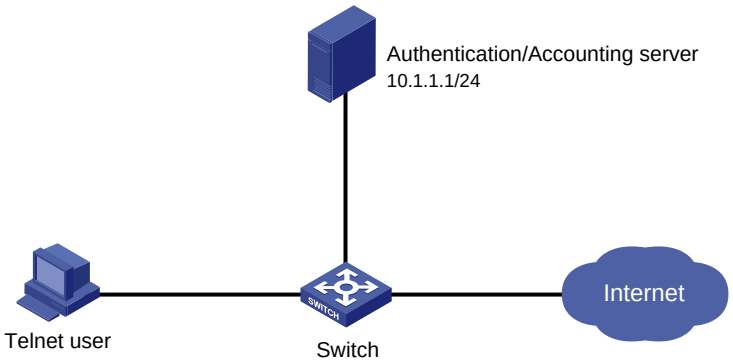
## AAA for Telnet Users by a HWTACACS Server

### Network requirements

As shown in Figure 1-7, configure the switch to use the HWTACACS server to provide authentication, authorization, and accounting services to login users.

- The HWTACACS server is used for authentication, authentication, and accounting. Its IP address is 10.1.1.1.
- On the switch, set the shared keys for authentication, authorization, and accounting packets to **expert**. Configure the switch to remove the domain name from a user name before sending the user name to the HWTACACS server.
- On the HWTACACS server, set the shared keys for packets exchanged with the switch to **expert**.

**Figure 1-7** Configure AAA for Telnet users by a HWTACACS server




### Configuration procedure

# Configure the IP addresses of the interfaces (omitted).

# Enable the Telnet server on the switch.

```
<Switch> system-view
[Switch] telnet server enable
```

# Configure the switch to use AAA for Telnet users.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
```

# Configure the HWTACACS scheme.

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49
[Switch-hwtacacs-hwtac] key authentication expert
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] key accounting expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

# Configure the AAA methods for the domain.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
```

# You can achieve the same result by setting default AAA methods for all types of users.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication default hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization default hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting default hwtacacs-scheme hwtac
```

When telneting into the switch, a user enters username userid@bbb for authentication using domain **bbb**.

## AAA for Telnet Users by Separate Servers

### Network requirements

As shown in Figure 1-8, configure the switch to provide local authentication, HWTACACS authorization, and RADIUS accounting services to Telnet users. The user name and the password for Telnet users are both **hello**.

- The HWTACACS server is used for authorization. Its IP address is 10.1.1.2. On the switch, set the shared keys for packets exchanged with the HWTACACS server to **expert**. Configure the switch to remove the domain name from a user name before sending the user name to the HWTACACS server.
- The RADIUS server is used for accounting. Its IP address is 10.1.1.1. On the switch, set the shared keys for packets exchanged with the RADIUS server to **expert**.

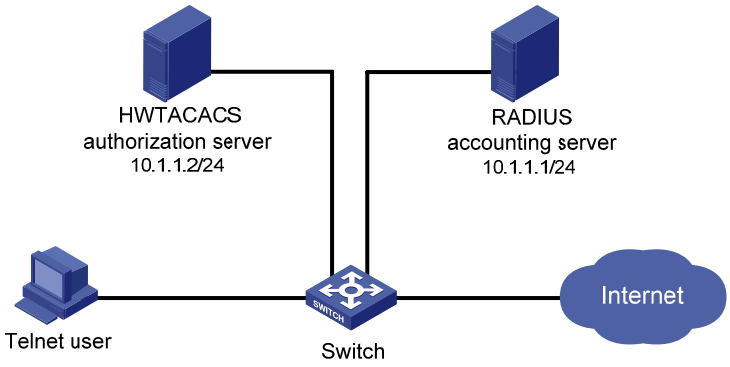
---

**Note**

Configuration of separate AAA for other types of users is similar to that given in this example. The only difference lies in the access type.

---

**Figure 1-8** Configure AAA by separate servers for Telnet users




## Configuration procedure

# Configure the IP addresses of various interfaces (omitted).

# Enable the Telnet server on the switch.

```
<Switch> system-view
[Switch] telnet server enable
```

# Configure the switch to use AAA for Telnet users.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
```

# Configure the HWTACACS scheme.

```
[Switch] hwtacacs scheme hwtac
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

# Configure the RADIUS scheme.

```
[Switch] radius scheme rd
[Switch-radius-rd] primary accounting 10.1.1.1 1813
[Switch-radius-rd] key accounting expert
[Switch-radius-rd] server-type extended
[Switch-radius-rd] user-name-format without-domain
[Switch-radius-rd] quit
```

# Create a local user named **hello**.

```
[Switch] local-user hello
[Switch-luser-hello] service-type telnet
[Switch-luser-hello] password simple hello
[Switch-luser-hello] quit
```

# Configure the AAA methods for the ISP domain.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login radius-scheme rd
```

```
[Switch-isp-bbb] quit
```

# Configure the default AAA methods for all types of users.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication default local
[Switch-isp-bbb] authorization default hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting default radius-scheme cams
```

When telneting into the switch, a user enters username telnet@bbb for authentication using domain **bbb**.

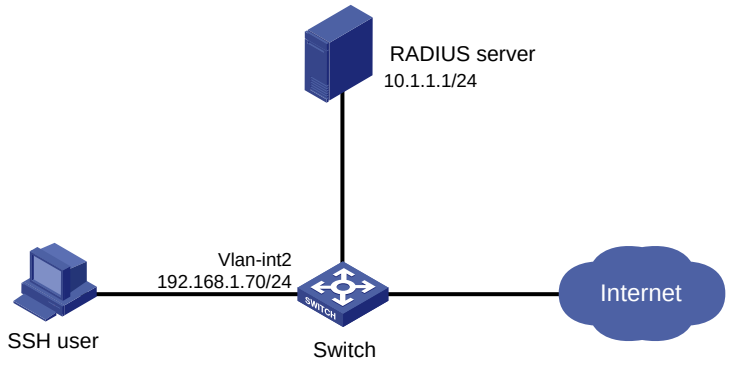
## AAA for SSH Users by a RADIUS Server

### Network requirements

As shown in Figure 1-9, configure the switch to use the RADIUS server to provide authentication, authorization, and accounting services to SSH users.

- The RADIUS server is responsible for both authentication and accounting. Its IP address is 10.1.1.1.
- On the switch, set both the shared keys for authentication and accounting packets to **expert**; and specify that the usernames sent to the RADIUS server carry the domain name.
- The RADIUS server runs the CAMS server.

**Figure 1-9** Configure AAA for SSH users by a RADIUS server




### Configuration procedure

1) Configure the RADIUS server.

---

**Note**

This example assumes that the RADIUS server runs the CAMS server Version 2.10.

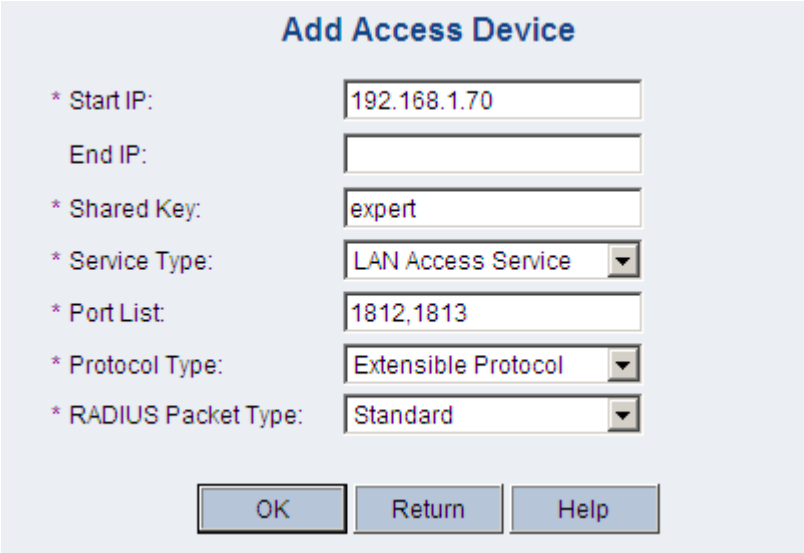
---

# Add an access device.

Log into the CAMS management platform and select **System Management** > **System Configuration** from the navigation tree. In the **System Configuration** window, click **Modify** of the **Access Device** item, and then click **Add** to enter the **Add Access Device** window and perform the following configurations:

- Specify the IP address of the switch as 192.168.1.70
- Set both the shared keys for authentication and accounting packets to **expert**
- Select **LAN Access Service** as the service type
- Specify the ports for authentication and accounting as 1812 and 1813 respectively
- Select **Extensible Protocol** as the protocol type
- Select **Standard** as the RADIUS packet type

**Figure 1-10** Add an access device

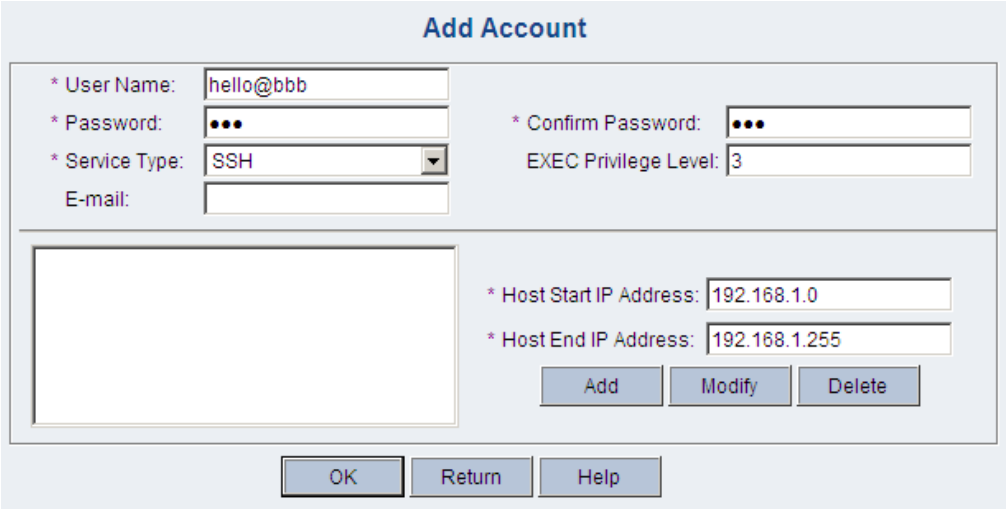



# Add a user for device management

From the navigation tree, select **User Management** > **User for Device Management**, and then in the right pane, click **Add** to enter the **Add Account** window and perform the following configurations:

- Add a user named **hello@bbb**, and specify the password
- Select **SSH** as the service type
- Specify the IP address range of the hosts to be managed

**Figure 1-11** Add an account for device management




2) Configure the switch

# Configure the IP address of VLAN interface 2, through which the SSH user accesses the switch.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

# Generate RSA and DSA key pairs and enable the SSH server.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# Configure the switch to use AAA for SSH users.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

# Configure the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

# Configure the RADIUS scheme.

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 10.1.1.1 1812
[Switch-radius-rad] primary accounting 10.1.1.1 1813
[Switch-radius-rad] key authentication expert
[Switch-radius-rad] key accounting expert
[Switch-radius-rad] user-name-format with-domain
[Switch-radius-rad] quit
```

# Configure the AAA methods for the domain.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login radius-scheme rad
[Switch-isp-bbb] quit
```

When using SSH to log in, a user enters a username in the form userid@bbb for authentication using domain **bbb**.

3) Verify the configuration

After the above configuration, the SSH user should be able to use the configured account to access the user interface of the switch. The commands that the user can access depend on the settings for EXEC users on the CAMS server.

# Troubleshooting AAA

## Troubleshooting RADIUS

**Symptom 1:** User authentication/authorization always fails.

**Analysis:**

1) A communication failure exists between the NAS and the RADIUS server.
2) The username is not in the format of userid@isp-name or no default ISP domain is specified for the NAS.

3) The user is not configured on the RADIUS server.
4) The password of the user is incorrect.
5) The RADIUS server and the NAS are configured with different shared key.

**Solution:**

Check that:

1) The NAS and the RADIUS server can ping each other.
2) The username is in the userid@isp-name format and a default ISP domain is specified on the NAS.
3) The user is configured on the RADIUS server.
4) The correct password is entered.
5) The same shared key is configured on both the RADIUS server and the NAS.

**Symptom 2:** RADIUS packets cannot reach the RADIUS server.

**Analysis:**

1) The communication link between the NAS and the RADIUS server is down (at the physical layer and data link layer).
2) The NAS is not configured with the IP address of the RADIUS server.
3) The UDP ports for authentication/authorization and accounting are not correct.
4) The port numbers of the RADIUS server for authentication, authorization and accounting are being used by other applications.

**Solution:**

Check that:

1) The communication links between the NAS and the RADIUS server work well at both physical and link layers.
2) The IP address of the RADIUS server is correctly configured on the NAS.
3) UDP ports for authentication/authorization/accounting configured on the NAS are the same as those configured on the RADIUS server.
4) The port numbers of the RADIUS server for authentication, authorization and accounting are available.

**Symptom 3:** A user is authenticated and authorized, but accounting for the user is not normal.

**Analysis:**

1) The accounting port number is not correct.
2) Configuration of the authentication/authorization server and the accounting server are not correct on the NAS. For example, one server is configured on the NAS to provide all the services of authentication/authorization and accounting, but in fact the services are provided by different servers.

**Solution:**

Check that:

1) The accounting port number is correctly set.
2) The authentication/authorization server and the accounting server are correctly configured on the NAS.

## Troubleshooting HWTACACS

Refer to Troubleshooting RADIUS if you encounter a HWTACACS fault.

# Table of Contents

# 1 802.1X Configuration

When configuring 802.1X, go to these sections for information you are interested in:



## 802.1X Overview

The 802.1X protocol was proposed by IEEE802 LAN/WAN committee for security of wireless LANs (WLAN). It has been widely used on Ethernet as a common port access control mechanism.

As a port-based access control protocol, 802.1X authenticates and controls accessing devices at the port level. A device connected to an 802.1X-enabled port of an access control device can access the resources on the LAN only after passing authentication.

**Note**

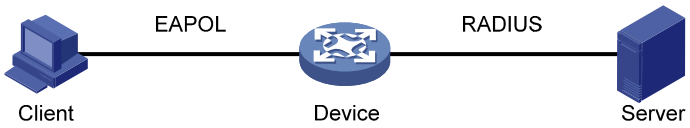
The port security feature provides rich security modes that combine or extend 802.1X and MAC address authentication. In a networking environment that requires flexible use of 802.1X and MAC address authentication, you are recommended to configure the port security feature. In a network environment that requires only 802.1X authentication, you are recommended to configure the 802.1X directly rather than configure the port security feature for simplicity sake. For how to use the port security feature, refer to *Port Security Configuration* in the *Security Volume*.

To get more information about 802.1X, go to these topics:

## Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: client, device, and server, as shown in Figure 1-1.

**Figure 1-1** Architecture of 802.1X




- Client: An entity to be authenticated by the device residing on the same LAN. A client is usually a user-end device and initiates 802.1X authentication through 802.1X client software supporting the EAP over LANs (EAPOL) protocol.
- Device: The entity that authenticates connected clients residing on the same LAN. A device is usually an 802.1X-enabled network device and provides ports (physical or logical) for clients to access the LAN.
- Server: The entity providing authentication, authorization, and accounting services for the device. The server usually runs the Remote Authentication Dial-in User Service (RADIUS).

## Authentication Modes of 802.1X

The 802.1X authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the client, device, and authentication server.

- Between the client and the device, EAP protocol packets are encapsulated using EAPOL to be transferred on the LAN.
- Between the device and the RADIUS server, EAP protocol packets can be handled in two modes: EAP relay and EAP termination. In EAP relay mode, EAP protocol packets are encapsulated by using the EAP over RADIUS (EAPOR) and then relayed to the RADIUS server. In EAP termination mode, EAP protocol packets are terminated at the device, repackaged in the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) attributes of RADIUS packets, and then transferred to the RADIUS server.

## Basic Concepts of 802.1X

These basic concepts are involved in 802.1X: controlled port/uncontrolled port, authorized state/unauthorized state, and control direction.

### Controlled port and uncontrolled port

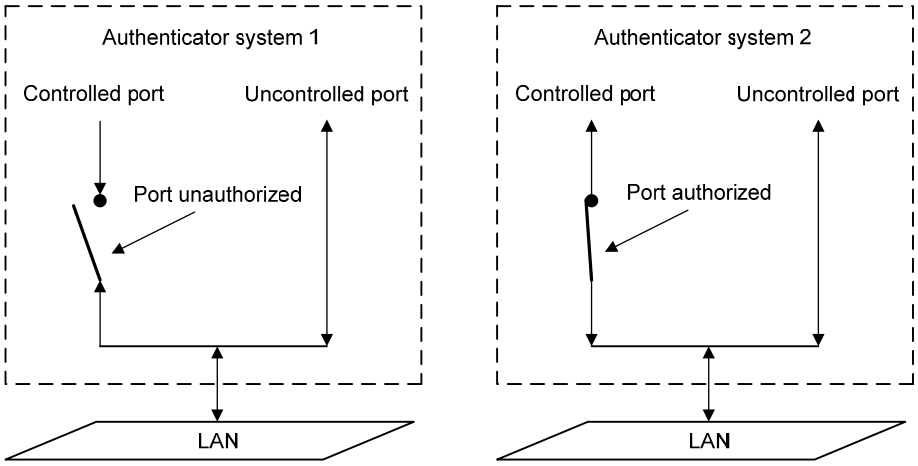
A device provides ports for clients to access the LAN. Each port can be regarded as a unity of two logical ports: a controlled port and an uncontrolled port.

- The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol frames to pass, guaranteeing that the client can always send and receive authentication frames.
- The controlled port is open to allow data traffic to pass only when it is in the authorized state.
- The controlled port and uncontrolled port are two parts of the same port. Any frames arriving at the port are visible to both of them.

### Authorized state and unauthorized state

The device uses the authentication server to authenticate a client trying to access the LAN and controls the status of the controlled port depending on the authentication result, putting the controlled port in the authorized state or unauthorized state, as shown in Figure 1-2.

**Figure 1-2** Authorized/unauthorized status of a controlled port




You can set the access control mode of a specified port to control the authorization status. The access control modes include:

- **authorized-force**: Places the port in the authorized state, allowing users of the ports to access the network without authentication.
- **unauthorized-force**: Places the port in the unauthorized state, denying any access requests from users of the ports.
- **auto**: Places the port in the unauthorized state initially to allow only EAPOL frames to pass, and turns the ports into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

### Control direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the client or just the traffic from the client.

---

**Note**

Currently, your device can only be set to deny traffic from the client.

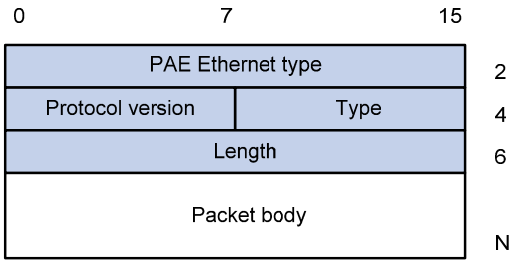
---

## EAP over LANs

### EAPOL frame format

EAPOL, defined in 802.1X, is intended to carry EAP protocol packets between clients and devices over LANs. Figure 1-3 shows the EAPOL frame format.

**Figure 1-3** EAPOL frame format




- PAE Ethernet type: Protocol type. It takes the value 0x888E.
- Protocol version: Version of the EAPOL protocol supported by the EAPOL frame sender.
- Type: Type of the EAPOL frame. Table 1-1 lists the types that the device currently supports.

**Table 1-1** Types of EAPOL frames

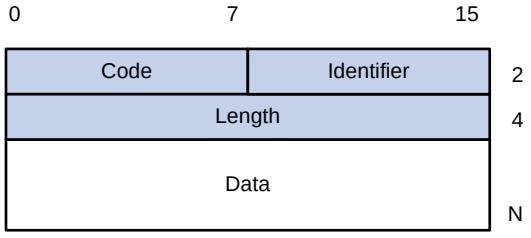
| Type | Description |
|---|---|
| EAP-Packet (a value of 0x00) | Frame for carrying authentication information, present between a device and the authentication server.<br>A frame of this type is repackaged and transferred by RADIUS to get through complex networks to reach the authentication server. |
| EAPOL-Start (a value of 0x01) | Frame for initiating authentication, present between a client and a device. |
| EAPOL-Logoff (a value of 0x02) | Frame for logoff request, present between a client and a device. |

- Length: Length of the data, that is, length of the Packet body field, in bytes. If the value of this field is 0, no subsequent data field is present.
- Packet body: Content of the packet. The format of this field varies with the value of the Type field.

## EAP Packet Format

An EAPOL frame of the type of EAP-Packet carries an EAP packet in its Packet body field. The format of the EAP packet is shown in Figure 1-4.

**Figure 1-4** EAP packet format

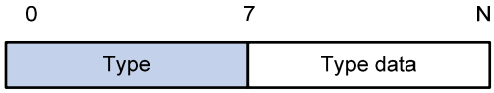



- Code: Type of the EAP packet, which can be Request, Response, Success, or Failure.

An EAP packet of the type of Success or Failure has no Data field, and has a length of 4.

An EAP packet of the type of Request or Response has a Data field in the format shown in Figure 1-5. The Type field indicates the EAP authentication type. A value of 1 represents Identity, indicating that the packet is for querying the identity of the client. A value of 4 represents MD5-Challenge, which corresponds closely to the PPP CHAP protocol.

**Figure 1-5** Format of the Data field in an EAP request/response packet




- Identifier: Allows matching of responses with requests.
- Length: Length of the EAP packet, including the Code, Identifier, Length, and Data fields, in bytes.
- Data: Content of the EAP packet. This field is zero or more bytes and its format is determined by the Code field.

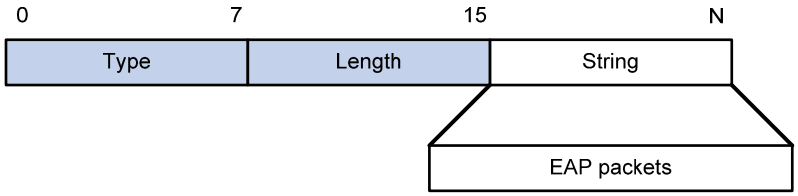
## EAP over RADIUS

Two attributes of RADIUS are intended for supporting EAP authentication: EAP-Message and Message-Authenticator. For information about RADIUS packet format, refer to *AAA Configuration* in the *Security Volume*.

### EAP-Message

The EAP-Message attribute is used to encapsulate EAP packets. Figure 1-6 shows its encapsulation format. The value of the Type field is 79. The String field can be up to 253 bytes. If the EAP packet is longer than 253 bytes, it can be fragmented and encapsulated into multiple EAP-Message attributes.

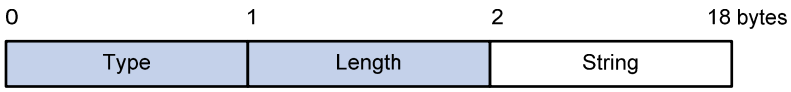
**Figure 1-6** Encapsulation format of the EAP-Message attribute




### Message-Authenticator

Figure 1-7 shows the encapsulation format of the Message-Authenticator attribute. The Message-Authenticator attribute is used to prevent access requests from being snooped during EAP or CHAP authentication. It must be included in any packet with the EAP-Message attribute; otherwise, the packet will be considered invalid and get discarded.

**Figure 1-7** Encapsulation format of the Message-Authenticator attribute




## 802.1X Authentication Triggering

802.1X authentication can be initiated by either a client or the device.

### Unsolicited triggering of a client

A client initiates authentication by sending an EAPOL-Start frame to the device. The destination address of the frame is 01-80-C2-00-00-03, the multicast address specified by the IEEE 802.1X protocol.

Some devices in the network may not support multicast packets with the above destination address, causing the authentication device unable to receive the authentication request of the client. To solve the problem, the device also supports EAPOL-Start frames whose destination address is a broadcast MAC address. In this case, the H3C iNode 802.1X client is required.

### Unsolicited triggering of the device

The device can trigger authentication by sending EAP-Request/Identity packets to unauthenticated clients periodically (every 30 seconds by default). This method can be used to authenticate clients which cannot send EAPOL-Start frames and therefore cannot trigger authentication, for example, the 802.1X client provided by Windows XP.

## Authentication Process of 802.1X

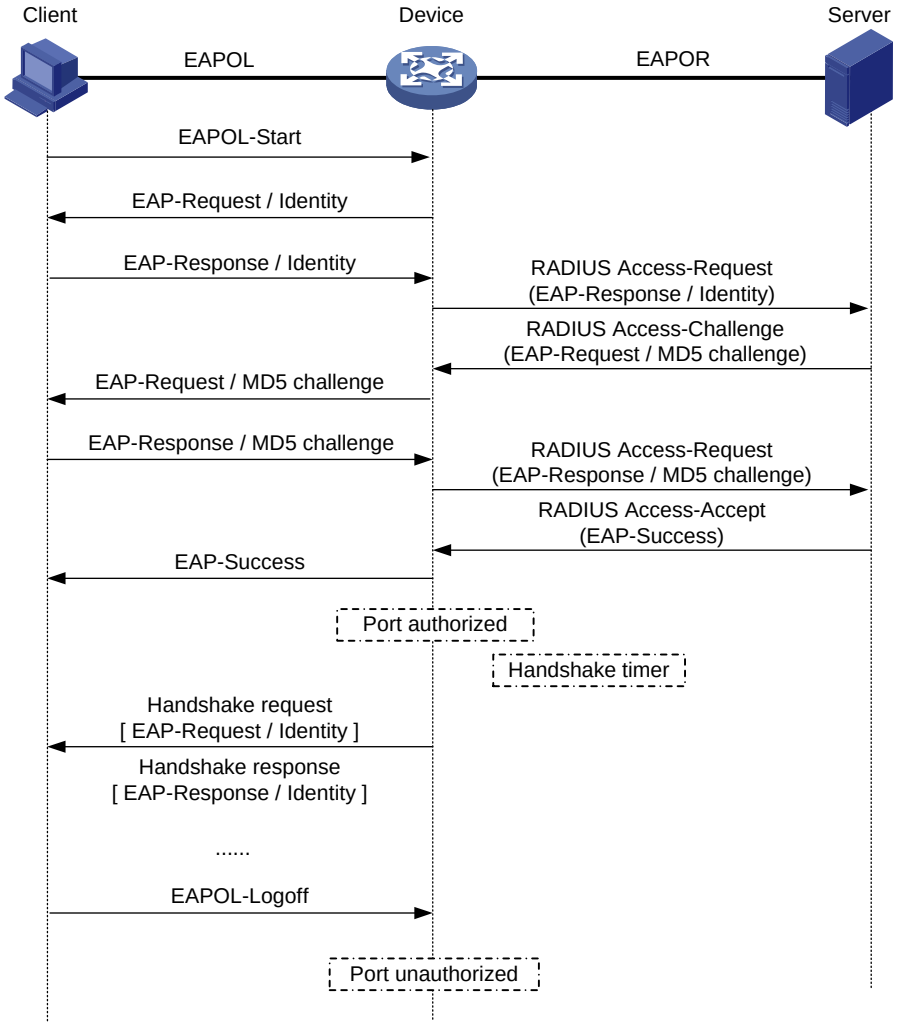
An 802.1X device communicates with a remotely located RADIUS server in two modes: EAP relay and EAP termination. The following description takes the EAP relay as an example to show the 802.1X authentication process.

### EAP relay

EAP relay is an IEEE 802.1X standard mode. In this mode, EAP packets are carried in an upper layer protocol, such as RADIUS, so that they can go through complex networks and reach the authentication server. Generally, EAP relay requires that the RADIUS server support the EAP attributes of EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying the EAP-Message attribute respectively.

Figure 1-8 shows the message exchange procedure with EAP-MD5.

**Figure 1-8** Message exchange in EAP relay mode




1) When a user launches the 802.1X client software and enters the registered username and password, the 802.1X client software generates an EAPOL-Start frame and sends it to the device to initiate an authentication process.
2) Upon receiving the EAPOL-Start frame, the device responds with an EAP-Request/Identity packet for the username of the client.
3) When the client receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the device.
4) Upon receiving the EAP-Response/Identity packet, the device relays the packet in a RADIUS Access-Request packet to the authentication server.
5) When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the device.
6) After receiving the RADIUS Access-Challenge packet, the device relays the contained EAP-Request/MD5 Challenge packet to the client.
7) When receiving the EAP-Request/MD5 Challenge packet, the client uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the device.
8) After receiving the EAP-Response/MD5 Challenge packet, the device relays the packet in a RADIUS Access-Request packet to the authentication server.

9) When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the device a RADIUS Access-Accept packet.
10) Upon receiving the RADIUS Access-Accept packet, the device opens the port to grant the access request of the client. After the client gets online, the device periodically sends handshake requests to the client to check whether the client is still online. By default, if two consecutive handshake attempts end up with failure, the device concludes that the client has gone offline and performs the necessary operations, guaranteeing that the device always knows when a client goes offline.
11) The client can also send an EAPOL-Logoff frame to the device to go offline unsolicitedly. In this case, the device changes the status of the port from authorized to unauthorized and sends an EAP-Failure frame to the client.

---

**Note**

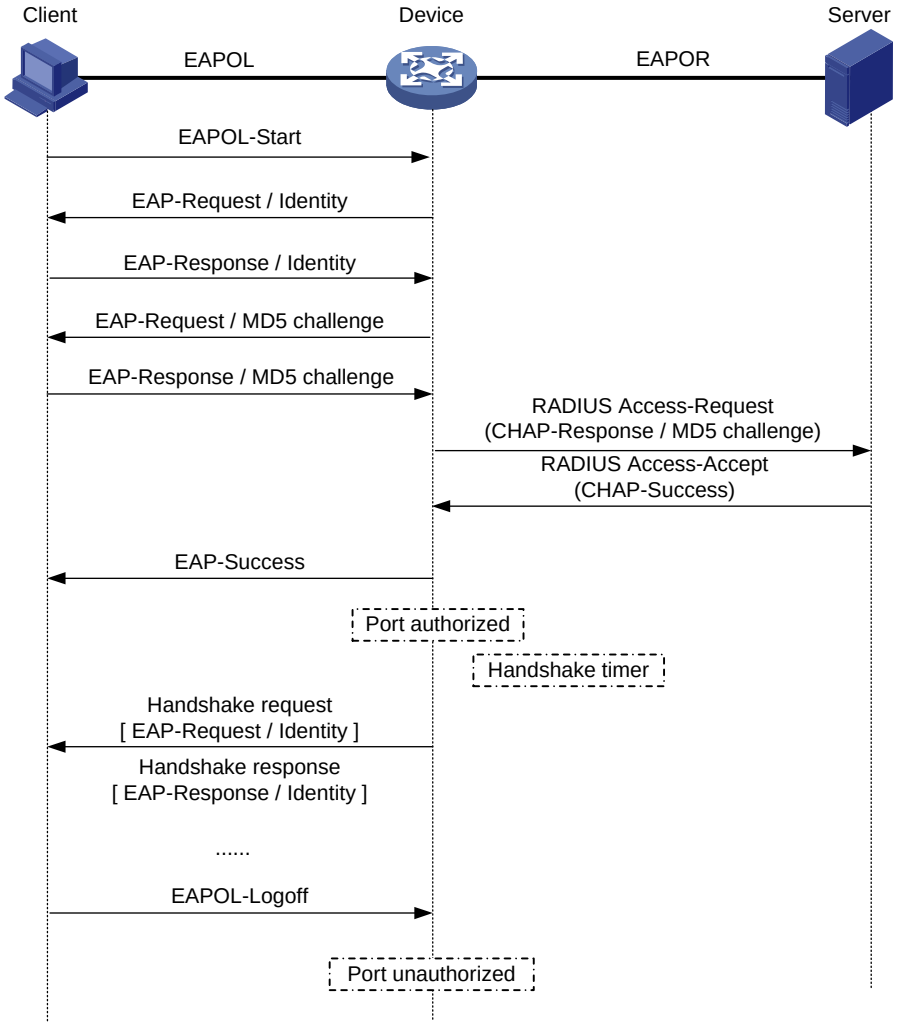
In EAP relay mode, a client must use the same authentication method as that of the RADIUS server. On the device, however, you only need to execute the **dot1x authentication-method eap** command to enable EAP relay.

---

### EAP termination

In EAP termination mode, EAP packets are terminated at the device and then repackaged into the PAP or CHAP attributes of RADIUS and transferred to the RADIUS server for authentication, authorization, and accounting. Figure 1-9 shows the message exchange procedure with CHAP authentication.

**Figure 1-9** Message exchange in EAP termination mode




Different from the authentication process in EAP relay mode, it is the device that generates the random challenge for encrypting the user password information in EAP termination authentication process. Consequently, the device sends the challenge together with the username and encrypted password information from the client to the RADIUS server for authentication.

## 802.1X Timers

This section describes the timers used on an 802.1X device to guarantee that the client, the device, and the RADIUS server can interact with each other in a reasonable manner.

- Username request timeout timer (tx-period): The device starts this timer when it sends an EAP-Request/Identity frame to a client. If it receives no response before this timer expires, the device retransmits the request. When cooperating with a client that sends EAPOL-Start requests only when requested, the device multicasts EAP-Request/Identity frames to the client at an interval set by this timer.
- Client timeout timer (supp-timeout): Once a device sends an EAP-Request/MD5 Challenge frame to a client, it starts this timer. If this timer expires but it receives no response from the client, it retransmits the request.
- Server timeout timer (server-timeout): Once a device sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.

- Handshake timer (handshake-period): After a client passes authentication, the device sends to the client handshake requests at this interval to check whether the client is online. If the device receives no response after sending the allowed maximum number of handshake requests, it considers that the client is offline.
- Quiet timer (quiet-period): When a client fails the authentication, the device refuses further authentication requests from the client in this period of time.

## Extensions to 802.1X

The devices extend and optimize the mechanism that the 802.1X protocol specifies by:

- Allowing multiple users to access network services through the same physical port.
- Supporting two authentication methods: **portbased** and **macbased**. With the **portbased** method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time. With the **macbased** method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

---

**Note**

After an 802.1X client passes authentication, the authentication server sends authorization information to the device. If the authorization information contains VLAN authorization information, the device adds the port connecting the client to the assigned VLAN. This neither changes nor affects the configurations of the port. The only result is that the assigned VLAN takes precedence over the manually configured one, that is, the assigned VLAN takes effect. After the client goes offline, the configured one takes effect.

---

## Features Working Together with 802.1X

### VLAN assignment

After an 802.1X user passes the authentication, the server will send an authorization message to the device. If the server is enabled with the VLAN assignment function, the assigned VLAN information will be included in the message. The device, depending on the link type of the port used to log in, adds the port to the assigned VLAN according to the following rules:

- If the port link type is Access, the port leaves its initial VLAN, that is, the VLAN configured for it and joins the assigned VLAN.
- If the port link type is Trunk, the assigned VLAN is allowed to pass the current trunk port. The default VLAN ID of the port is that of the assigned VLAN.
- If the port link type is Hybrid, the assigned VLAN is allowed to pass the current port without carrying the tag. The default VLAN ID of the port is that of the assigned VLAN. Note that if the Hybrid port is assigned a MAC-based VLAN, the device will dynamically create a MAC-based VLAN according to the VLAN assigned by the authentication server, and remain the default VLAN ID of the port unchanged.

The assigned VLAN neither changes nor affects the configuration of a port. However, as the assigned VLAN has higher priority than the initial VLAN of the port, it is the assigned VLAN that takes effect after a user passes authentication. After the user goes offline, the port returns to the initial VLAN of the port.

For details about VLAN configuration, refer to *VLAN Configuration* in the *Access Volume*.

---

**Note**

- With a Hybrid port, the VLAN assignment will fail if you have configured the assigned VLAN to carry tags.
- With a Hybrid port, you cannot configure an assigned VLAN to carry tags after the VLAN has been assigned.

---

### Guest VLAN

Guest VLAN allows unauthenticated users and users failing the authentication to access a specified VLAN, where the users can, for example, download or upgrade the client software, or execute some user upgrade programs. This VLAN is called the guest VLAN.

Currently, on the S4500G series Ethernet switches, a guest VLAN can be only a port-based guest VLAN (PGV), which is supported on a port that uses the access control method of **portbased**.

With PGV configured on a port, if no users are successfully authenticated on the port in a certain period of time (90 seconds by default), the port will be added to the guest VLAN and all users accessing the port will be authorized to access the resources in the guest VLAN.

The device adds a PGV-configured port into the guest VLAN according to the port's link type in the similar way as described in VLAN assignment. When a user of a port in the guest VLAN initiates an authentication, if the authentication is not successful, the port stays in the guest VLAN; if the authentication is successful, the port leaves the guest VLAN, and:

- If the authentication server assigns a VLAN, the port joins the assigned VLAN. After the user goes offline, the port returns to its initial VLAN, that is, the VLAN specified for it during port configuration, or, in other words, the VLAN it was in before it joined the guest VLAN.
- If the authentication server does not assign any VLAN, the port returns to its initial VLAN. After the client goes offline, the port just stays in its initial VLAN.

### ACL assignment

ACLs provide a way of controlling access to network resources and defining access rights. When a user logs in through a port, and the RADIUS server is configured with authorization ACLs, the device will permit or deny data flows traversing through the port according to the authorization ACLs. Before specifying authorization ACLs on the server, you need to configure the ACL rules on the device. You can change the access rights of users by modifying authorization ACL settings on the RADIUS server or changing the corresponding ACL rules on the device.

### Mandatory authentication domain for a specified port

The mandatory authentication domain function provides a security control mechanism for 802.1X access. With a mandatory authentication domain specified for a port, the system uses the mandatory

authentication domain for authentication, authorization, and accounting of all 802.1X users on the port. In this way, users accessing the port cannot use any account in other domains.

Meanwhile, for EAP relay mode 802.1X authentication that uses certificates, the certificate of a user determines the authentication domain of the user. However, you can specify different mandatory authentication domains for different ports even if the user certificates are from the same certificate authority (that is, the user domain names are the same). This allows you to deploy 802.1X access policies flexibly.

# Configuring 802.1X

## Configuration Prerequisites

802.1X provides a user identity authentication scheme. However, 802.1X cannot implement the authentication scheme solely by itself. RADIUS or local authentication must be configured to work with 802.1X.

- Configure the ISP domain to which the 802.1X user belongs and the AAA scheme to be used (that is, local authentication or RADIUS).
- For remote RADIUS authentication, the username and password information must be configured on the RADIUS server.
- For local authentication, the username and password information must be configured on the device and the service type must be set to **lan-access**.

For detailed configuration of the RADIUS client, refer to *AAA Configuration* in the *Security Volume*.

## Configuring 802.1X Globally

Follow these steps to configure 802.1X globally:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable 802.1X globally | | **dot1x** | Required<br>Disabled by default |
| Set the authentication method | | **dot1x authentication-method** { **chap** \| **eap** \| **pap** } | Optional<br>CHAP by default |
| Set the port access control parameters | Set the port access control mode for specified or all ports | **dot1x port-control** { **authorized-force** \| **auto** \| **unauthorized-force** } [ **interface** *interface-list* ] | Optional<br>**auto** by default |
| | Set the port access control method for specified or all ports | **dot1x port-method** { **macbased** \| **portbased** } [ **interface** *interface-list* ] | Optional<br>**macbased** by default |
| | Set the maximum number of users for specified or all ports | **dot1x max-user** *user-number* [ **interface** *interface-list* ] | Optional<br>256 by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the maximum number of attempts to send an authentication request to a client | **dot1x retry** *max-retry-value* | Optional<br>2 by default |
| Set timers | **dot1x timer** { **handshake-period** *handshake-period-value* \| **quiet-period** *quiet-period-value* \| **server-timeout** *server-timeout-value* \| **supp-timeout** *supp-timeout-value* \| **tx-period** *tx-period-value* } | Optional<br>The defaults are as follows:<br>15 seconds for the handshake timer,<br>60 seconds for the quiet timer,<br>100 seconds for the server timeout timer,<br>30 seconds for the client timeout timer, and<br>30 seconds for the username request timeout timer. |
| Enable the quiet timer | **dot1x quiet-period** | Optional<br>Disabled by default |

Note that:

- For 802.1X to take effect on a port, you must enable it both globally in system view and for the port in system view or Ethernet interface view.
- You can also enable 802.1X and set port access control parameters (that is, the port access control mode, port access method, and the maximum number of users) for a port in Ethernet interface view. For detailed configuration, refer to Configuring 802.1X for a Port. The only difference between configuring 802.1X globally and configuring 802.1X for a port lies in the applicable scope. If both a global setting and a local setting exist for an argument of a port, the last configured one is in effect.
- 802.1X timers only need to be changed in special or extreme network environments. For example, you can give the client timeout timer a higher value in a low-performance network, give the quiet timer a higher value in a vulnerable network or a lower value for quicker authentication response, or adjust the server timeout timer to suit the performance of the authentication server.

## Configuring 802.1X for a Port

### Enabling 802.1X for a port

Follow these steps to enable 802.1X for a port:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable 802.1X for one or more ports | In system view | **dot1x interface** *interface-list* | Required<br>Use either approach.<br>Disabled by default |
| | In Ethernet interface view | **interface** *interface-type interface-number* | |
| | | **dot1x** | |

### Configuring 802.1X parameters for a port

Follow these steps to configure 802.1X parameters for a port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Set the port access control mode for the port | **dot1x port-control** { **authorized-force** \| **auto** \| **unauthorized-force** } | Optional<br>**auto** by default |
| Set the port access control method for the port | **dot1x port-method** { **macbased** \| **portbased** } | Optional<br>**macbased** by default |
| Set the maximum number of users for the port | **dot1x max-user** *user-number* | Optional<br>256 by default |
| Enable online user handshake | **dot1x handshake** | Optional<br>Enabled by default |
| Enable multicast trigger | **dot1x multicast-trigger** | Optional<br>Enabled by default |
| Specify the mandatory authentication domain for the port | **dot1x mandatory-domain** *domain-name* | Optional<br>No mandatory authentication domain is specified by default. |

Note that:

- Enabling 802.1X on a port is mutually exclusive with adding the port to an aggregation group.
- In EAP relay authentication mode, the device encapsulates the 802.1X user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication. In this case, you can configure the **user-name-format** command but it does not take effect. For information about the **user-name-format** command, refer to *AAA Commands* in the *Security Volume.*
- If the username of a client contains the version number or one or more blank spaces, you can neither retrieve information nor disconnect the client by using the username. However, you can use items such as IP address and connection index number to do so.
- Once enabled with the 802.1X multicast trigger function, a port sends multicast trigger messages to the client periodically to initiate authentication.
- For a user-side device sending untagged traffic, the voice VLAN function and 802.1X are mutually exclusive and cannot be configured together on the same port. For details about voice VLAN, refer to *VLAN Configuration* in the *Access Volume*.

# Configuring an 802.1X Port-based Guest VLAN

## Configuration prerequisites

- Enable 802.1X.
- Create the VLAN to be specified as the guest VLAN.
- Set the port access control method to **portbased**.
- Ensure that the 802.1X multicast trigger function is enabled.

## Configuration procedure

Follow these steps to configure a port-based guest VLAN:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Configure the guest VLAN for specified or all ports | In system view | **dot1x guest-vlan** *guest-vlan-id* [ **interface** *interface-list* ] | Required<br>Use either approach.<br>By default, a port is configured with no guest VLAN. |
| | In Ethernet interface view | **interface** *interface-type interface-number*<br>**dot1x guest-vlan** *vlan-id* | |

**Note**

- Different ports can be configured with different guest VLANs, but a port can be configured with only one guest VLAN.
- You cannot configure both the guest VLAN function and the free IP function in EAD fast deployment.

**Caution**

If the data flows from a user-side device carry VLAN tags, and 802.1X and guest VLAN are enabled on the access port, you are recommended to configure different VLAN IDs for the voice VLAN, the default port VLAN, and the guest VLAN of 802.1X.

# Displaying and Maintaining 802.1X

| To do… | Use the command… | Remarks |
|---|---|---|
| Display 802.1X session information, statistics, or configuration information of specified or all ports | **display dot1x** [ **sessions** \| **statistics** ] [ **interface** *interface-list* ] | Available in any view |
| Clear 802.1X statistics | **reset dot1x statistics** [ **interface** *interface-list* ] | Available in user view |

# 802.1X Configuration Example

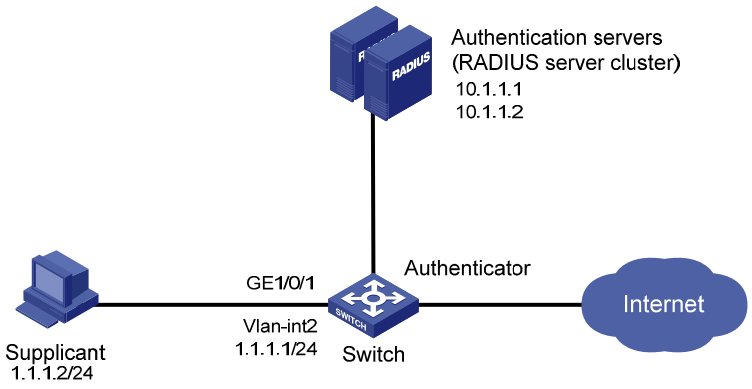
## Network requirements

- The access control method of **macbased** is required on the port GigabitEthernet 1/0/1 to control clients.
- All clients belong to default domain aabbcc.net, which can accommodate up to 30 users. RADIUS authentication is performed at first, and then local authentication when no response from the RADIUS server is received. If the RADIUS accounting fails, the device gets users offline.
- A server group with two RADIUS servers is connected to the device. The IP addresses of the servers are 10.1.1.1 and 10.1.1.2 respectively. Use the former as the primary

authentication/secondary accounting server, and the latter as the secondary authentication/primary accounting server.

- Set the shared key for the device to exchange packets with the authentication server as name, and that for the device to exchange packets with the accounting server as money.
- Specify the device to try up to five times at an interval of 5 seconds in transmitting a packet to the RADIUS server until it receives a response from the server, and to send real time accounting packets to the accounting server every 15 minutes.
- Specify the device to remove the domain name from the username before passing the username to the RADIUS server.
- Set the username of the 802.1X user as **localuser** and the password as **localpass** and specify to use clear text mode. Enable the idle cut function to get the user offline whenever the user remains idle for over 20 minutes.

**Figure 1-10** Network diagram for 802.1X configuration




## Configuration procedure

**Note**

The following configuration procedure covers most AAA/RADIUS configuration commands for the device, while configuration on the 802.1X client and RADIUS server are omitted. For information about AAA/RADIUS configuration commands, refer to *AAA Configuration* in the *Security Volume*.

# Configure the IP addresses for each interface. (Omitted)

# Add local access user localuser, enable the idle cut function, and set the idle cut interval.

```
<Device> system-view
[Device] local-user localuser
[Device-luser-localuser] service-type lan-access
[Device-luser-localuser] password simple localpass
[Device-luser-localuser] attribute idle-cut 20
[Device-luser-localuser] quit
```

# Create RADIUS scheme **radius1** and enter its view.

```
[Device] radius scheme radius1
```

# Configure the IP addresses of the primary authentication and accounting RADIUS servers.

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.2
```

# Configure the IP addresses of the secondary authentication and accounting RADIUS servers.

```
[Device-radius-radius1] secondary authentication 10.1.1.2
[Device-radius-radius1] secondary accounting 10.1.1.1
```

# Specify the shared key for the device to exchange packets with the authentication server.

```
[Device-radius-radius1] key authentication name
```

# Specify the shared key for the device to exchange packets with the accounting server.

```
[Device-radius-radius1] key accounting money
```

# Set the interval for the device to retransmit packets to the RADIUS server and the maximum number of transmission attempts.

```
[Device-radius-radius1] timer response-timeout 5
[Device-radius-radius1] retry 5
```

# Set the interval for the device to send real time accounting packets to the RADIUS server.

```
[Device-radius-radius1] timer realtime-accounting 15
```

# Specify the device to remove the domain name of any username before passing the username to the RADIUS server.

```
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

# Create domain **aabbcc.net** and enter its view.

```
[Device] domain aabbcc.net
```

# Set **radius1** as the RADIUS scheme for users of the domain and specify to use local authentication as the secondary scheme.

```
[Device-isp-aabbcc.net] authentication default radius-scheme radius1 local
[Device-isp-aabbcc.net] authorization default radius-scheme radius1 local
[Device-isp-aabbcc.net] accounting default radius-scheme radius1 local
```

# Set the maximum number of users for the domain as 30.

```
[Device-isp-aabbcc.net] access-limit enable 30
```

# Enable the idle cut function and set the idle cut interval.

```
[Device-isp-aabbcc.net] idle-cut enable 20
[Device-isp-aabbcc.net] quit
```

# Configure **aabbcc.net** as the default domain.

```
[Device] domain default enable aabbcc.net
```

# Enable 802.1X globally.

```
[Device] dot1x
```

# Enable 802.1X for port GigabitEthernet 1/0/1.

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
```

# Set the port access control method. (Optional. The default settings meet the requirement.)

```
[Device] dot1x port-method macbased interface GigabitEthernet 1/0/1
```

# Guest VLAN and VLAN Assignment Configuration Example

## Network requirements

As shown in Figure 1-11:

- A host is connected to port GigabitEthernet 1/0/2 of the device and must pass 802.1X authentication to access the Internet. GigabitEthernet 1/0/2 is in VLAN 1.
- The authentication server runs RADIUS and is in VLAN 2.
- The update server, which is in VLAN 10, is for client software download and upgrade.
- Port GigabitEthernet 1/0/3 of the device, which is in VLAN 5, is for accessing the Internet.

As shown in Figure 1-12:

- On port GigabitEthernet 1/0/2, enable 802.1X and set VLAN 10 as the guest VLAN of the port. If the device sends an EAP-Request/Identity packet from the port for the maximum number of times but still receives no response, the device adds the port to its guest VLAN. In this case, the host and the update server are both in VLAN 10, so that the host can access the update server and download the 802.1X client.

As shown in Figure 1-13:

- After the host passes the authentication and logs in, the host is added to VLAN 5. In this case, the host and GigabitEthernet 1/0/3 are both in VLAN 5, so that the host can access the Internet.

**Figure 1-11** Network diagram for guest VLAN configuration

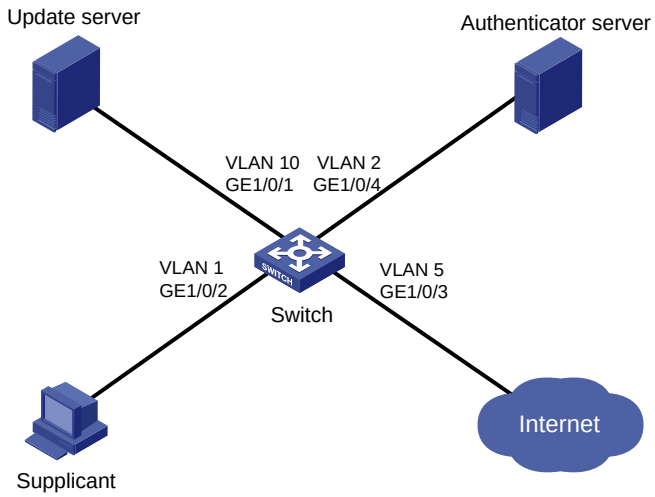


**Figure 1-12** Network diagram with the port in the guest VLAN

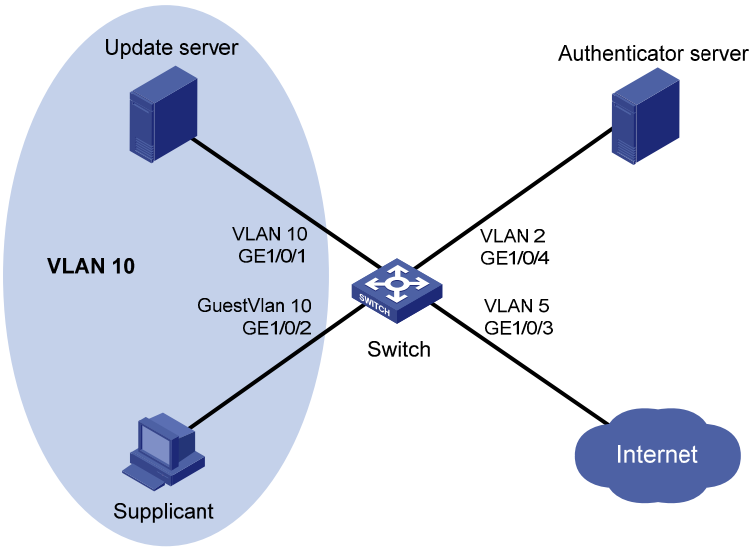
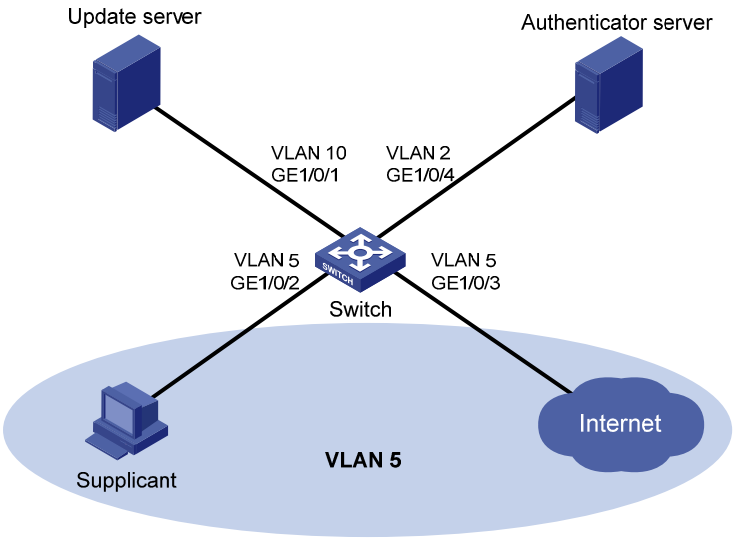



**Figure 1-13** Network diagram when the client passes authentication




## Configuration procedure

**Note**

- The following configuration procedure uses many AAA/RADIUS commands. For detailed configuration of these commands, refer to *AAA Configuration* in the *Security Volume*.
- Configurations on the 802.1X client and RADIUS server are omitted.

# Configure RADIUS scheme 2000.

```
<Device> system-view
[Device] radius scheme 2000
```

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
[Device-radius-2000] primary accounting 10.11.1.1 1813
[Device-radius-2000] key authentication abc
[Device-radius-2000] key accounting abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

# Configure authentication domain **system** and specify to use RADIUS scheme 2000 for users of the domain.

```
[Device] domain system
[Device-isp-system] authentication default radius-scheme 2000
[Device-isp-system] authorization default radius-scheme 2000
[Device-isp-system] accounting default radius-scheme 2000
[Device-isp-system] quit
```

# Enable 802.1X globally.

```
[Device] dot1x
```

# Enable 802.1X for port GigabitEthernet 1/0/2.

```
[Device] interface GigabitEthernet 1/0/2
[Device-GigabitEthernet1/0/2] dot1x
```

# Set the port access control method to **portbased**.

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

# Set the port access control mode to **auto**.

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
[Device-GigabitEthernet1/0/2] quit
```

# Create VLAN 10.

```
[Device] vlan 10
[Device-vlan10] quit
```

# Specify port GigabitEthernet 1/0/2 to use VLAN 10 as its guest VLAN.

```
[Device] dot1x guest-vlan 10 interface GigabitEthernet 1/0/2
```

You can use the **display current-configuration** or **display interface GigabitEthernet 1/0/2** command to view your configuration. You can also use the **display vlan 10** command in the following cases to verify whether the configured guest VLAN functions:

- When no users log in.
- When a user fails the authentication.
- When a user goes offline.

After a user passes the authentication successfully, you can use the **display interface GigabitEthernet 1/0/2** command to verity that port GigabitEthernet 1/0/2 has been added to the assigned VLAN 5.

# ACL Assignment Configuration Example

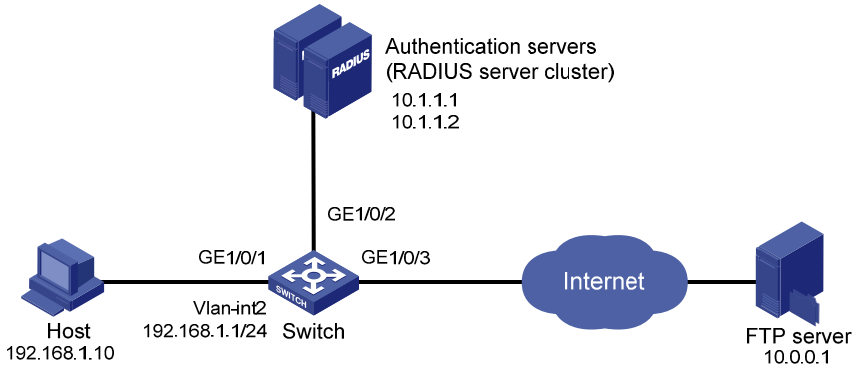
## Network requirements

As shown in Figure 1-14, a host is connected to port GigabitEthernet 1/0/1 of the device and must pass 802.1X authentication to access the Internet.

- Configure the RADIUS server to assign ACL 3000.
- Enable 802.1X authentication on port GigabitEthernet 1/0/1 of the device, and configure ACL 3000.

After the host passes 802.1X authentication, the RADIUS server assigns ACL 3000 to port GigabitEthernet 1/0/1. As a result, the host can access the Internet but cannot access the FTP server, whose IP address is 10.0.0.1.

**Figure 1-14** Network diagram for ACL assignment




## Configuration procedure

# Configure the IP addresses of the interfaces. (Omitted)

# Configure the RADIUS scheme.

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication abc
[Device-radius-2000] key accounting abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

# Create an ISP domain and specify the AAA schemes.

```
[Device] domain 2000
[Device-isp-2000] authentication default radius-scheme 2000
[Device-isp-2000] authorization default radius-scheme 2000
[Device-isp-2000] accounting default radius-scheme 2000
[Device-isp-2000] quit
```

# Configure ACL 3000 to deny packets destined for 10.0.0.1.

```
[Device] acl number 3000
[Device-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
```

# Enable 802.1X globally.

```
[Device] dot1x
```

# Enable 802.1X for port GigabitEthernet 1/0/1.

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

After logging in successfully, a user can use the **ping** command to verify whether the ACL 3000 assigned by the RADIUS server functions.

```
[Device] ping 10.0.0.1
  PING 10.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.0.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

# 2 EAD Fast Deployment Configuration

When configuring EAD fast deployment, go to these sections for information you are interested in:



## EAD Fast Deployment Overview

### Overview

Endpoint Admission Defense (EAD) is an integrated endpoint access control solution. By allowing the security clients, access devices, security policy servers, and third-party servers in the network to collaborate with each other, it can improve the overall defense capability of a network and implement centralized management of users.

Normally, to use EAD on your network, you need to manually deploy the EAD client on each device, which tends to be time consuming and inefficient. To address the issue, quick EAD deployment was developed. In conjunction with 802.1X, it can have an access switch to force all attached devices to download and install the EAD client before permitting them to access the network.

### EAD Fast Deployment Implementation

To support the fast deployment of EAD schemes, 802.1X provides the following two mechanisms:

1) Limit on accessible network resources

Before successful 802.1X authentication, a user can access only a specific IP segment, which may have one or more servers. Users can download EAD client software or obtain dynamic IP address from the servers.

2) URL redirection

Before successful 802.1X authentication, a user using a Web browser to access the network is automatically redirected to a specified URL, for example, the EAD client software download page. The server that provides the URL redirection must be in the specific network segment that users can access before passing 802.1X authentication.

# Configuring EAD Fast Deployment

**Note**

Currently, MAC authentication and port security cannot work together with EAD fast deployment. Once MAC authentication or port security is enabled globally, the EAD fast deployment is disabled automatically.

## Configuration Prerequisites

- Enable 802.1X globally.
- Enable 802.1X on the specified port, and set the access control mode to **auto**.

## Configuration Procedure

### Configuring a freely accessible network segment

A freely accessible network segment, also called a free IP, is a network segment that users can access before passing 802.1X authentication.

Once a free IP is configured, the fast deployment of EAD is enabled.

Follow these steps to configure a freely accessible network segment:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a freely accessible network segment | **dot1x free-ip** *ip-address* { *mask-address* \| *mask-length* } | Required<br>No freely accessible network segment is configured by default. |

**Note**

- You cannot configure both the free IP and the 802.1X guest VLAN function.
- If no freely accessible network segment is configured, a user cannot obtain a dynamic IP address before passing 802.1X authentication. To solve this problem, you can configure a freely accessible network segment that is on the same network segment with the DHCP server.

### Configuring the IE redirect URL

Follow these steps to configure the IE redirect URL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the IE redirect URL | **dot1x url** *url-string* | Required<br>No redirect URL is configured by default. |

**Note**

The redirect URL and the freely accessible network segment must belong to the same network segment. Otherwise, the specified URL is unaccessible.

### Setting the EAD rule timeout time

With the EAD fast deployment function, a user is authorized by an EAD rule (generally an ACL rule) to access the freely accessible network segment before passing authentication. After successful authentication, the occupied ACL will be released. If a large amount of users access the freely accessible network segment but fail the authentication, ACLs will soon be used up and new users will be rejected.

An EAD rule timeout timer is designed to solve this problem. When a user accesses the network, this timer is started. If the user neither downloads client software nor performs authentication before the timer expires, the occupied ACL will be released so that other users can use it. When there are a large number of users, you can shorten the timeout time to improve the ACL usage efficiency.

Follow these steps to set the EAD rule timeout time:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set EAD rule timeout time | **dot1x timer ead-timeout** *ead-timeout-value* | Optional<br>30 minutes by default |

## Displaying and Maintaining EAD Fast Deployment

| To do… | Use the command… | Remarks |
|---|---|---|
| Display 802.1X session information, statistics, or configuration information | **display dot1x** [ **sessions** \| **statistics** ] [ **interface** *interface-list* ] | Available in any view |

# EAD Fast Deployment Configuration Example

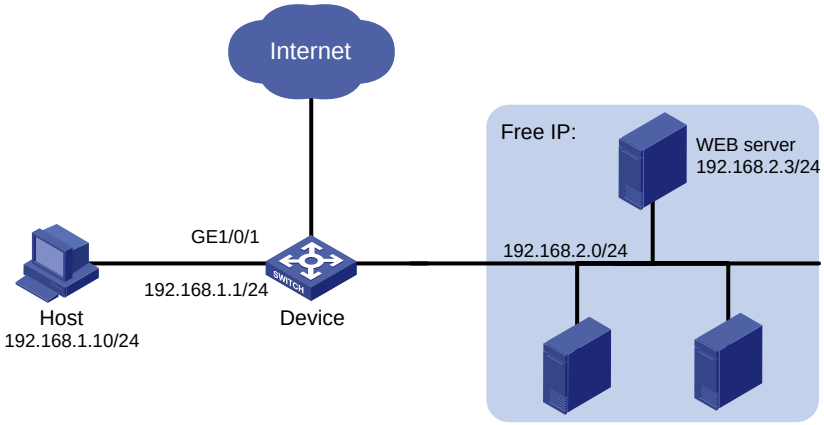
## Network requirements

As shown in Figure 2-1, the host is connected to the device, and the device is connected to the freely accessible network segment and outside network.

It is required that:

- Before successful 802.1 authentication, the host using IE to access outside network will be redirected to the WEB server, and it can download and install 802.1X client software.
- After successful 802.1X authentication, the host can access outside network.

**Figure 2-1** Network diagram for EAD fast deployment




## Configuration procedure

1) Configure the WEB server

Before using the EAD fast deployment function, you need to configure the WEB server to provide the download service of 802.1X client software.

2) Configure the device to support EAD fast deployment

# Configure the IP addresses of the interfaces (omitted).

# Configure the free IP.

```
<Device> system-view
[Device] dot1x free-ip 192.168.2.0 24
```

# Configure the redirect URL for client software download.

```
[Device] dot1x url http://192.168.2.3
```

# Enable 802.1X globally.

```
[Device] dot1x
```

# Enable 802.1X on the port.

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

3) Verify your configuration

# Use the **ping** command to ping an IP address within the network segment specified by free IP to check that the user can access that segment before passing 802.1X authentication.

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Besides, if the user uses IE to access any external website, the user will be taken to the WEB server, which provides the client software download service.

# Troubleshooting EAD Fast Deployment

## Users Cannot be Redirected Correctly

### Symptom

When a user enters an external website address in the IE browser, the user is not redirected to the specified URL.

### Analysis

- The address is in the string format. In this case, the operating system of the host regards the string a website name and tries to have it resolved. If the resolution fails, the operating system sends an ARP request with the address in the format other than X.X.X.X. The redirection function does redirect this kind of ARP request.
- The address is within the freely accessible network segment. In this case, the device regards that the user is trying to access a host in the freely accessible network segment, and redirection will not take place, even if no host is present with the address.
- The redirect URL is not in the freely accessible network segment, no server is present with that URL, or the server with the URL does not provide WEB services.

### Solution

- Enter an IP address that is not within the freely accessible network segment in dotted decimal notation (X.X.X.X).
- Ensure that the device and the server are configured correctly.

# Table of Contents

# 1 HABP Configuration

When configuring HABP, go to these sections for the information you are interested in:



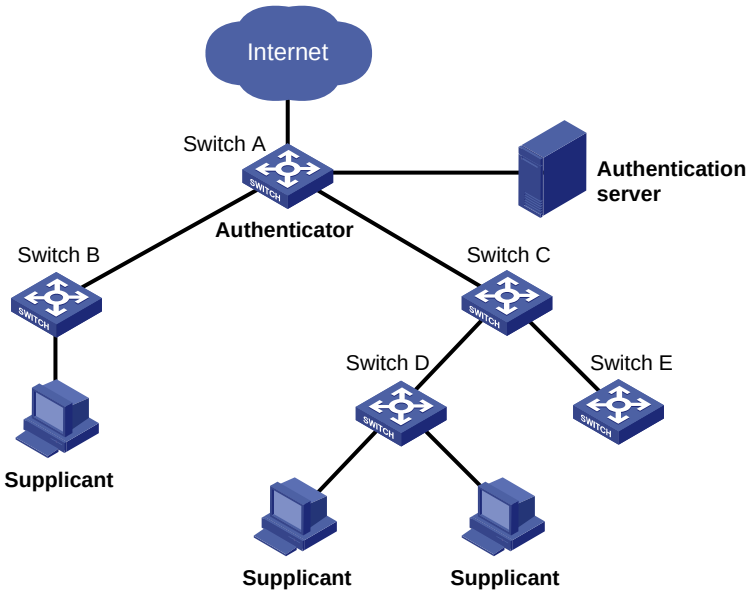
## Introduction to HABP

The HW Authentication Bypass Protocol (HABP) is used to enable the downstream network devices of an 802.1X or MAC authentication enabled access device to bypass 802.1X authentication and MAC authentication.

HABP is usually adopted at the access layer of a campus or enterprise network. This feature is useful when 802.1X authentication or MAC address authentication is adopted on the management switch of a cluster, in which case you must configure HABP to allow the packets between the member devices of the cluster to bypass 802.1X authentication because network devices usually do not support 802.1 client. Otherwise, the management device will fail to perform centralized management of the cluster member devices. For more information about the cluster function, refer to *Cluster Configuration* in the *System Volume*.

As shown in Figure 1-1, 802.1X authenticator Switch A has two switches attached to it: Switch B and Switch C. On Switch A, 802.1X authentication is enabled globally and on the ports connecting the downstream network devices. The end-user devices (the supplicants) run the 802.1X client software for 802.1X authentication. For Switch B and Switch D, where 802.1X client is not supported (which is typical of network devices), the communication between them will fail because they cannot pass 802.1X authentication and their packets will be blocked on Switch A. To allow the two switches to communicate, you can use HABP.

**Figure 1-1** Network diagram for HABP application




HABP is a link layer protocol that works above the MAC layer. It is built on the client-server model. Generally, the HABP server is assumed by the management device (such as Switch A in the above example), and the attached switches function as the HABP clients, such as Switch B through Switch E in the example. No device can function as both an HABP server and a client at the same time. Typically, the HABP server sends HABP requests to all its clients periodically to collect their MAC addresses, and the clients respond to the requests. After the server learns the MAC addresses of all the clients, it registers the MAC addresses as HABP entries. Then, link layer frames exchanged between the clients can bypass the 802.1X authentication on ports of the server without affecting the normal operation of the whole network. All HABP packets must travel in a VLAN, which is called the management VLAN. Communication between the HABP server and the HABP clients is implemented through the management VLAN.

# Configuring HABP

Complete the following tasks to configure HABP:

- Configuring the HABP Server
- Configuring an HABP Client

## Configuring the HABP Server

With the HABP server function enabled, the administrative device starts to send HABP requests to the attached switches. The HABP responses include the MAC addresses of the attached switches. This makes it possible for the administrative device to manage the attached switches.

You can configure the interval of sending HABP requests on the administrative device.

Follow these steps to configure an HABP server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable HABP | **habp enable** | Optional<br>Enabled by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure HABP to work in server mode | **habp server vlan** *vlan-id* | Required<br>HABP works in client mode by default. |
| Set the interval to send HABP requests | **habp timer** *interval* | Optional<br>20 seconds by default |

### Configuring an HABP Client

Configure the HABP client function on each device that is attached to the administrative device and needs to be managed. As the HABP client function is enabled by default, this configuration task is optional.

Follow these steps to configure an HABP client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable HABP | **habp enable** | Optional<br>Enabled by default |
| Configure HABP to work in client mode | **undo habp server** | Optional<br>HABP works in client mode by default. |

## Displaying and Maintaining HABP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display HABP configuration information | **display habp** | Available in any view |
| Display HABP MAC address table entries | **display habp table** | Available in any view |
| Display HABP packet statistics | **display habp traffic** | Available in any view |

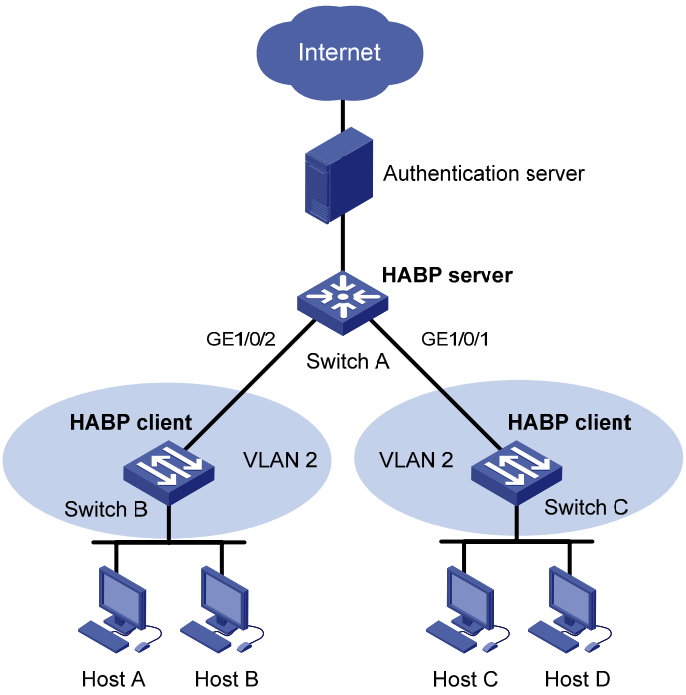
## HABP Configuration Example

### Network requirements

Switch A is the administrative device and connects two access devices: Switch B and Switch C. Configure HABP so that Switch A can manage Switch B and Switch C.

- Configure Switch A as the HABP server, allowing HABP packets to be transmitted in VLAN 2.
- Enable HABP client on Switch B and Switch C.
- On switch A, set the interval to send HABP request packets to 50 seconds.

**Figure 1-2** Network diagram for HABP configuration




## Configuration procedure

1) Configure Switch A

# Enable HABP.

```
<SwitchA> system-view
[SwitchA] habp enable
```

# Configure HABP to work in server mode, allowing HABP packets to be transmitted in VLAN 2.

```
[SwitchA] habp server vlan 2
```

# Set the interval to send HABP request packets to 50 seconds.

```
[SwitchA] habp timer 50
```

2) Configure Switch B and Switch C

Configure Switch B and Switch C to work in HABP client mode. This configuration is usually unnecessary because HABP is enabled and works in client mode by default.

3) Verify your configuration

# Display HABP configuration information.

```
<SwitchA> display habp
Global HABP information:
    HABP Mode: Server
    Sending HABP request packets every 50 seconds
    Bypass VLAN: 2
```

# Display HABP MAC address table entries.

```
<SwitchA> display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        GigabitEthernet 1/0/2
001f-3c00-0031  53        GigabitEthernet 1/0/1
```

# Table of Contents

# 1 MAC Authentication Configuration

When configuring MAC authentication, go to these sections for information you are interested in:



## MAC Authentication Overview

MAC authentication provides a way for authenticating users based on ports and MAC addresses. Once detecting a new MAC address, the device initiates the authentication process. MAC authentication requires neither client software to be installed on the hosts, nor any username or password to be entered by users during authentication.

Currently, the device supports two MAC authentication modes: Remote Authentication Dial-In User Service (RADIUS) based MAC authentication and local MAC authentication. For detailed information about RADIUS authentication and local authentication, refer to *AAA Configuration* of the *Security Volume*.

MAC authentication supports two types of usernames:

- MAC address, where the MAC address of a user serves as both the username and password.
- Fixed username, where all users use the same preconfigured username and password for authentication, regardless of the MAC addresses.

### RADIUS-Based MAC Authentication

In RADIUS-based MAC authentication, the device serves as a RADIUS client and requires a RADIUS server to cooperate with it.

- If the type of username is MAC address, the device forwards a detected MAC address as the username and password to the RADIUS server for authentication of the user.
- If the type of username is fixed username, the device sends the same username and password configured locally to the RADIUS server for authentication of each user.

If the authentication succeeds, the user will be granted permission to access the network resources.

### Local MAC Authentication

In local MAC authentication, the device performs authentication of users locally and different items need to be manually configured for users on the device according to the specified type of username:

- If the type of username is MAC address, a local user must be configured for each user on the device, using the MAC address of the accessing user as both the username and password.
- If the type of username is fixed username, a single username and optionally a single password are required for the device to authenticate all users.

# Related Concepts

## MAC Authentication Timers

The following timers function in the process of MAC authentication:

- Offline detect timer: At this interval, the device checks to see whether there is traffic from a user. Once detecting that there is no traffic from a user within this interval, the device logs the user out and sends to the RADIUS server a stop accounting request.
- Quiet timer: Whenever a user fails MAC authentication, the device does not perform MAC authentication of the user during such a period.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user to access the network.

## Quiet MAC Address

When a user fails MAC authentication, the MAC address becomes a quiet MAC address, which means that any packets from the MAC address will be discarded silently by the device until the quiet timer expires. This prevents the device from authenticating an illegal user repeatedly in a short time.

---

 **Caution**

If a quiet MAC address is the same as a static MAC address configured or an MAC address that has passed another type of authentication, the quiet function does not take effect.

---

## VLAN Assigning

For separation of users from restricted network resources, users and restricted resources are usually put into different VLANs. After a user passes identity authentication, the authorization server assigns to the user the VLAN where the restricted resources reside as an authorized VLAN, and the port through which the user accesses the device will be assigned to the authorized VLAN. As a result, the user can access those restricted network resources.

## ACL Assigning

ACLs assigned by an authorization server are referred to as authorization ACLs, which are designed to control access to network resources. If the RADIUS server is configured with authorization ACLs, the device will permit or deny data flows traversing through the port through which a user accesses the device according to the authorization ACLs. You can change access rights of users by modifying authorization ACL settings on the RADIUS server.

# Configuring MAC Authentication

## Configuration Prerequisites

- Create and configure an ISP domain.
- For local authentication, create the local users and configure the passwords.

- For RADIUS authentication, ensure that a route is available between the device and the RADIUS server, and add the usernames and passwords on the server.

**Caution**

When adding usernames and passwords on the device or server, ensure that:

- The type of username and password must be consistent with that used for MAC authentication.
- All the letters in the MAC address to be used as the username and password must be in lower case.
- The service type of the local users must be configured as **lan-access**.

## Configuration Procedure

Follow these steps to configure MAC authentication:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable MAC authentication globally | **mac-authentication** | Required<br>Disabled by default |
| Enable MAC authentication for specified ports | **mac-authentication interface** *interface-list* | Required<br>Use either approach.<br>Disabled by default |
| | **interface** *interface-type interface-number*<br>**mac-authentication**<br>**quit** | |
| Specify the ISP domain for MAC authentication | **mac-authentication domain** *isp-name* | Optional<br>The default ISP domain is used by default. |
| Set the offline detect timer | **mac-authentication timer offline-detect** *offline-detect-value* | Optional<br>300 seconds by default |
| Set the quiet timer | **mac-authentication timer quiet** *quiet-value* | Optional<br>60 seconds by default |
| Set the server timeout timer | **mac-authentication timer server-timeout** *server-timeout-value* | Optional<br>100 seconds by default |
| Configure the username and password for MAC authentication | **mac-authentication user-name-format** { **fixed** [ **account** *name* ] [ **password** { **cipher** \| **simple** } *password* ] \| **mac-address** [ **with-hyphen** \| **without-hyphen** ] } | Optional<br>By default, the user's source MAC address serves as the username and password, with "-" in the MAC address. |

**Note**

- You can configure MAC authentication for ports first. However, the configuration takes effect only after you enable MAC authentication globally.
- Enabling MAC authentication on a port is mutually exclusive with adding the port to an aggregation group.
- For details about the default ISP domain, refer to *AAA Configuration* in the *Security Volume*.

# Displaying and Maintaining MAC Authentication

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the global MAC authentication information or the MAC authentication information about specified ports | **display mac-authentication** [ **interface** *interface-list* ] | Available in any view |
| Clear the MAC authentication statistics | **reset mac-authentication statistics** [ **interface** *interface-list* ] | Available in user view |

# MAC Authentication Configuration Examples

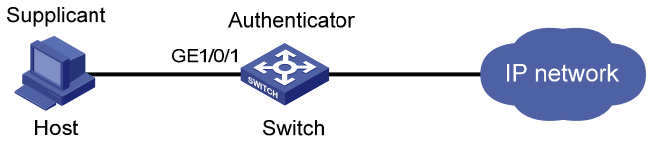
## Local MAC Authentication Configuration Example

### Network requirements

As illustrated in Figure 1-1, a supplicant is connected to the device through port GigabitEthernet 1/0/1.

- Local MAC authentication is required on every port to control user access to the Internet.
- All users belong to domain aabbcc.net.
- Local users use their MAC addresses as the usernames and passwords for authentication.
- Set the offline detect timer to 180 seconds and the quiet timer to 3 minutes.

**Figure 1-1** Network diagram for local MAC authentication




### Configuration procedure

1) Configure MAC authentication on the device

# Add a local user, setting the username and password as 00-e0-fc-12-34-56, the MAC address of the user.

```
<Device> system-view
[Device] local-user 00-e0-fc-12-34-56
[Device-luser-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
[Device-luser-00-e0-fc-12-34-56] service-type lan-access
```

```
[Device-luser-00-e0-fc-12-34-56] quit
```

# Configure ISP domain **aabbcc.net**, and specify that the users in the domain use local authentication.

```
[Device] domain aabbcc.net
[Device-isp-aabbcc.net] authentication lan-access local
[Device-isp-aabbcc.net] quit
```

# Enable MAC authentication globally.

```
[Device] mac-authentication
```

# Enable MAC authentication for port GigabitEthernet 1/0/1.

```
[Device] mac-authentication interface GigabitEthernet 1/0/1
```

# Specify the ISP domain for MAC authentication.

```
[Device] mac-authentication domain aabbcc.net
```

# Set the MAC authentication timers.

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

# Specify the MAC authentication username format as MAC address, that is, using the MAC address (with hyphens) of a user as the username and password for MAC authentication of the user.

```
[Device] mac-authentication user-name-format mac-address with-hyphen
```

2) Verify the configuration

# Display global MAC authentication information.

```
<Device> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 1
          Current domain is aabbcc.net
Silent Mac User info:
         MAC ADDR              From Port           Port Index
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Current online user number is 1
    MAC ADDR         Authenticate state           AuthIndex
    00e0-fc12-3456   MAC_AUTHENTICATOR_SUCCESS     29
```

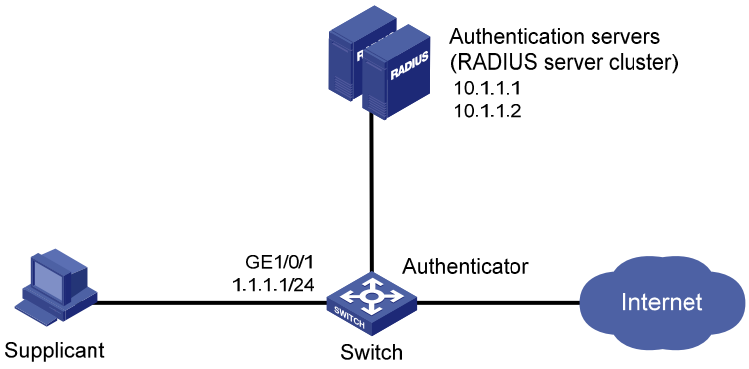
## RADIUS-Based MAC Authentication Configuration Example

### Network requirements

As illustrated in Figure 1-2, a host is connected to the device through port GigabitEthernet 1/0/1. The device authenticates, authorizes and keeps accounting on the host through the RADIUS server.

- MAC authentication is required on every port to control user access to the Internet.
- Set the offline detect timer to 180 seconds and the quiet timer to 3 minutes.
- All users belong to ISP domain 2000.
- The username type of fixed username is used for authentication, with the username being **aaa** and password being **123456**.

**Figure 1-2** Network diagram for MAC authentication using RADIUS




## Configuration procedure

**Note**

It is required that the RADIUS server and the device are reachable to each other and the username and password are configured on the server.

1) Configure MAC authentication on the device

# Configure a RADIUS scheme.

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication abc
[Device-radius-2000] key accounting abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

# Specify the AAA schemes for the ISP domain.

```
[Device] domain 2000
[Device-isp-2000] authentication default radius-scheme 2000
[Device-isp-2000] authorization default radius-scheme 2000
[Device-isp-2000] accounting default radius-scheme 2000
[Device-isp-2000] quit
```

# Enable MAC authentication globally.

```
[Device] mac-authentication
```

# Enable MAC authentication for port GigabitEthernet 1/0/1.

```
[Device] mac-authentication interface GigabitEthernet 1/0/1
```

# Specify the ISP domain for MAC authentication.

```
[Device] mac-authentication domain 2000
```

# Set the MAC authentication timers.

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

# Specify to use the username **aaa** and password 123456 for MAC authentication of all users.

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

2) Verify the configuration

# Display global MAC authentication information.

```
<Device> display mac-authentication
MAC address authentication is enabled.
User name format is fixed account
 Fixed username:aaa
 Fixed password:123456
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 1
          Current domain is 2000
Silent Mac User info:
         MAC ADDR              From Port           Port Index
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Current online user number is 1
    MAC ADDR         Authenticate state           AuthIndex
    00e0-fc12-3456   MAC_AUTHENTICATOR_SUCCESS     29
```

## ACL Assignment Configuration Example

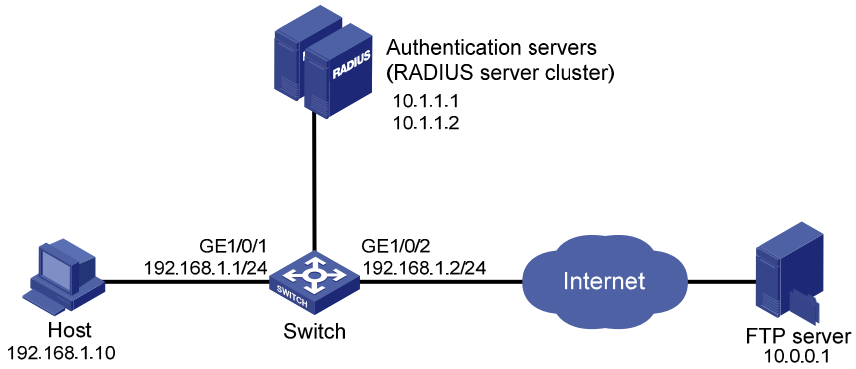
### Network requirements

As shown in Figure 1-3, a host is connected to port GigabitEthernet 1/0/1 of the switch and must pass MAC authentication to access the Internet.

- Specify to use the MAC address of a user as the username and password for MAC authentication of the user.
- Configure the RADIUS server to assign ACL 3000.
- On port GigabitEthernet 1/0/1 of the switch, enable MAC authentication and configure ACL 3000.

After the host passes MAC authentication, the RADIUS server assigns ACL 3000 to port GigabitEthernet 1/0/1 of the switch. As a result, the host can access the Internet but cannot access the FTP server, whose IP address is 10.0.0.1.

**Figure 1-3** Network diagram for ACL assignment




## Configuration procedure

**Note**

- Make sure that there is a route available between the RADIUS server and the switch.
- In this example, the switch uses the default username type (user MAC address) for MAC authentication. Therefore, you need to add the username and password of each user on the RADIUS server correctly.
- You need to configure the RADIUS server to assign ACL 3000 as the authorization ACL.

# Configure the RADIUS scheme.

```
<Sysname> system-view
[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.1.1.1 1812
[Sysname-radius-2000] primary accounting 10.1.1.2 1813
[Sysname-radius-2000] key authentication abc
[Sysname-radius-2000] key accounting abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit
```

# Create an ISP domain and specify the AAA schemes.

```
[Sysname] domain 2000
[Sysname-isp-2000] authentication default radius-scheme 2000
[Sysname-isp-2000] authorization default radius-scheme 2000
[Sysname-isp-2000] accounting default radius-scheme 2000
[Sysname-isp-2000] quit
```

# Configure ACL 3000 to deny packets destined for 10.0.0.1.

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Sysname-acl-adv-3000] quit
```

# Enable MAC authentication globally.

```
[Sysname] mac-authentication
```

# Specify the ISP domain for MAC authentication users.

```
[Sysname] mac-authentication domain 2000
```

# Specify the MAC authentication username type as MAC address, that is, using the MAC address of a user as the username and password for MAC authentication of the user.

```
[Sysname] mac-authentication user-name-format mac-address
```

# Enable MAC authentication for port GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

After completing the above configurations, you can use the **ping** command to verify whether the ACL 3000 assigned by the RADIUS server functions.

```
[Sysname] ping 10.0.0.1
  PING 10.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.0.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

# Table of Contents

# 1 Portal Configuration

When configuring portal, go to these sections for information you are interested in:



## Portal Overview

This section covers these topics:



### Introduction to Portal

Portal authentication, as its name implies, helps control access to the Internet. Portal authentication is also called web authentication and a website implementing portal authentication is called a portal website.

With portal authentication, an access device forces all users to log into the portal website at first. Every user can access the free services provided on the portal website; but to access the Internet, a user must pass portal authentication on the portal website.

A user can access a known portal website, enter username and password for authentication. This authentication mode is called active authentication. There is still another authentication mode, namely forced authentication, in which the access device forces a user trying to access the Internet through HTTP to log in to a portal website for authentication.

The portal feature provides the flexibility for Internet service providers (ISPs) to manage services. A portal website can, for example, present advertisements, and deliver community services and personalized services. In this way, broadband network providers, equipment providers, and content service providers form an industrial ecological system.

### Introduction to Extended Portal Functions

By forcing users to implement patching and anti-virus policies, extended portal functions help users to defend against viruses. The main extended functions are described as follows:

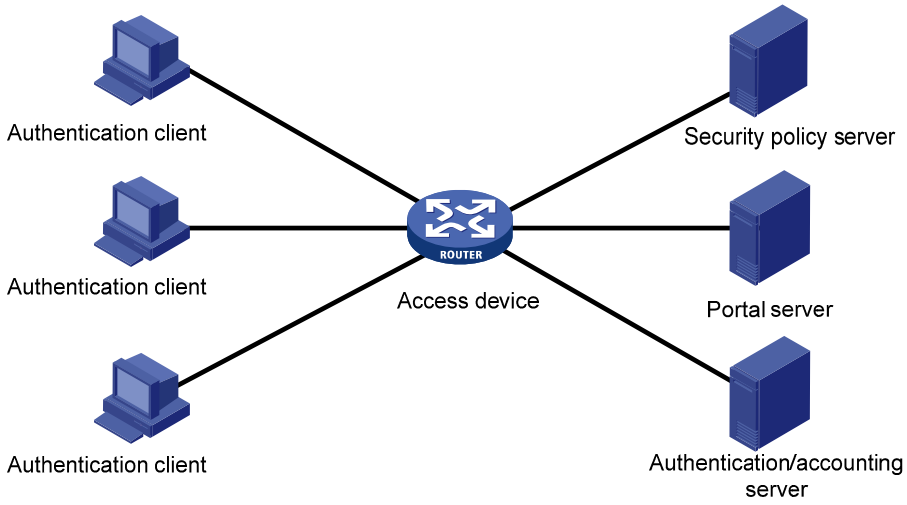
- Security authentication mechanism: The security authentication mechanism works after the identity authentication process to check that the required anti-virus software, virus definition updates and OS patches are installed, and no unauthorized software is installed on the terminal of a user.

- Resource access limit: A user passing identity authentication can access only network resources like the anti-virus server or OS patch server, which are called the restricted resources. Only users passing security authentication can access more network resources, which are called the unrestricted resources.

## Portal System Components

As shown in Figure 1-1, a typical portal system consists of five basic components: authentication client, access device, portal server, authentication/accounting server, and security policy server.

**Figure 1-1** Portal system components




### Authentication client

Client system of a user to be authenticated. It can be a browser using the Hypertext Transfer Protocol (HTTP/HTTPS), or a host running the portal client software. The security authentication of a client depends on the communications between the portal client and the security policy server.

### Access device

Device for broadband access. It can be a switch or a router that provides the following three functions:

- Before authentication, redirecting all HTTP requests from users in the subnet to be authenticated to the portal server.
- During authentication, interacting with the portal server, security policy server and the authentication/accounting server for identity authentication, security authentication and accounting.
- After authentication, allowing users to access granted Internet resources.

### Portal server

Server that listens to authentication requests from portal clients and exchanges client authentication information with the access device. It provides free portal services and a web-based authentication interface.

### Authentication/accounting server

Server that implements user authentication and accounting through interaction with the access device.

### Security policy server

Server that interacts with portal clients and access devices for security authentication and resource authorization.

The above five components interact in the following procedure:

1) When an unauthenticated user enters a website address in the address bar of the IE to access the Internet, an HTTP request is created and sent to the access device, which redirects the HTTP request to the web authentication homepage of the portal server. For extended portal functions, authentication clients must run the portal client.
2) On the authentication homepage/authentication dialog box, the user enters and submits the authentication information, which the portal server then transfers to the access device.
3) Upon receipt of the authentication information, the access device communicates with the authentication/accounting server for authentication and accounting.
4) After successful authentication, the access device checks whether there is corresponding security policy for the user. If not, it allows the user to access the Internet. Otherwise, the client, the access device and the security policy server communicates to perform security authentication of the user, and the security policy server authorizes the user to access resources depending on the security authentication result.

---

**Note**

- Since a portal client uses an IP address as its ID, ensure that there is no Network Address Translation (NAT) device between the authentication client, access device, portal server, and authentication/accounting server when deploying portal authentication. This is to avoid authentication failure due to NAT operations.
- Currently, only a RADIUS server can serve as the authentication/accounting server in a portal system.
- Currently, security authentication requires the cooperation of the H3C iNode client.

---

## Portal Authentication Modes

Portal authentication supports two modes: non-Layer 3 authentication and Layer 3 authentication.

### Non-Layer 3 authentication

Non-Layer 3 authentication falls into two categories: direct authentication and Re-DHCP authentication.

- Direct authentication

Before authentication, a user manually configures an IP address or directly obtains a public IP address through DHCP, and can access only the portal server and predefined free websites. After passing authentication, the user can access the network resources. The process of direct authentication is simpler than that of re-DHCP authentication.

- Re-DHCP authentication

Before authentication, a user gets a private IP address through DHCP and can access only the portal server and predefined free websites. After passing authentication, the user is allocated a public IP address and can access the network resources. No public IP address is allocated to those who fails

authentication. This solves the problem about IP address planning and allocation and proves to be useful. For example, a service provider can allocate public IP addresses to broadband users only when they access networks beyond the residential community network.

### Layer 3 authentication

Layer 3 portal authentication is similar to direct authentication. However, in Layer-3 portal authentication mode, Layer 3 forwarding devices can be present between the authentication client and the access device.

### Differences between Layer 3 and non-Layer 3 authentication modes

- Networking mode

From this point of view, the difference between these two authentication modes lies in whether or not a Layer 3 forwarding device can be present between the authentication client and the access device. The former supports Layer 3 forwarding devices, while the latter does not.

- User identifier

In Layer 3 authentication mode, a client is uniquely identified by an IP address. This is because the mode supports Layer 3 forwarding devices between the authentication client and the access device but the access device does not learn the MAC address of the authentication client. In non-Layer 3 authentication mode, a client is uniquely identified by the combination of its IP address and MAC address because the access device can learn the MAC address of the authentication client.

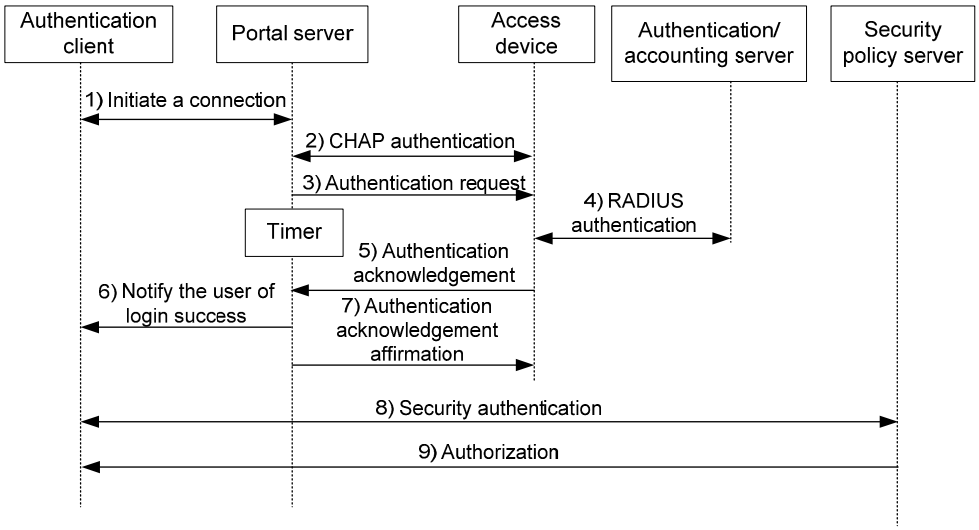
Due to the above differences, when the MAC address of an authentication client remains the same but the IP address changes, a new portal authentication will be triggered in Layer-3 authentication mode but will not be triggered in non-Layer 3 authentication mode. In non-Layer 3 authentication mode, a new portal authentication will be triggered only when both the MAC and IP address of the authentication client are changed.

## Portal Authentication Process

Direct authentication and Layer 3 authentication share the same authentication process, while re-DHCP authentication has a different process because of the presence of two address allocation procedures.

## Direct authentication/Layer 3 authentication process

**Figure 1-2** Direct authentication/Layer 3 authentication process




The direct authentication/Layer 3 authentication process is as follows:

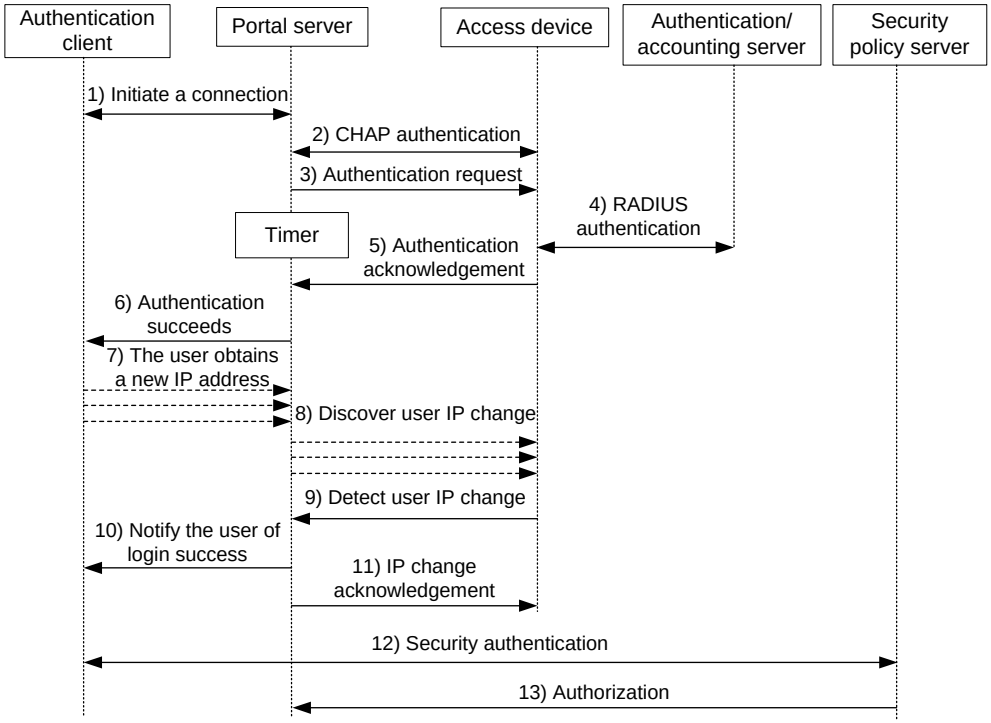
1) A portal user initiates an authentication request through HTTP. When the HTTP packet arrives at the access device, the access device allows it to pass if it is destined for the portal server or a predefined free website, or redirects it to the portal server if it is destined for other websites. The portal server provides a web page for the user to enter the username and password.
2) The portal server and the access device exchange Challenge Handshake Authentication Protocol (CHAP) messages. For Password Authentication Protocol (PAP) authentication, this step is skipped.
3) The portal server assembles the username and password into an authentication request message and sends it to the access device. Meanwhile, the portal server starts a timer to wait for an authentication acknowledgment message.
4) The access device and the RADIUS server exchange RADIUS packets to authenticate the user.
5) If the user passes authentication, the access device sends an authentication acknowledgment message to the portal server.
6) The portal server sends an authentication acknowledgment message to the authentication client to notify it of logon success.
7) The portal server sends an affirmation message to the access device.

With extended portal functions, the process includes two additional steps:

8) The security policy server exchanges security authentication information with the client to check whether the authentication client meets the security requirements.
9) The security policy server authorizes the user to access unrestricted resources based on the security configuration for the user. The authorization information is stored on the access device and used by the access device to control user access.

### Re-DHCP authentication process

**Figure 1-3** Re-DHCP authentication process




The re-DHCP authentication process is as follows:

Step 1 through step 6 are the same as those in the direct authentication/Layer 3 portal authentication process.

7) After receiving an authentication acknowledgment message, the authentication client obtains a new public IP address through DHCP and notifies the portal server that it has obtained a public IP address.
8) The portal server notifies the access device that the authentication client has obtained a new public IP address.
9) Detecting the change of the IP address by examining ARP packets received, the access device notifies the portal server of the change.
10) The portal server notifies the authentication client of logon success.
11) The portal server sends a user IP address change acknowledgment message to the access device.

With extended portal functions, the process includes two additional steps:

12) The security policy server exchanges security authentication information with the client to check whether the authentication client meets the security requirements.
13) The security policy server authorizes the user to access unrestricted resources based on the security configuration for the user. The authorization information is stored on the access device and used by the access device to take control of user access.

## Portal Configuration Task List

Complete these tasks to configure portal authentication:

| Task | Remarks |
|---|---|
| Basic Portal Configuration | Required |
| Configuring a Portal-Free Rule | Optional |
| Configuring an Authentication Subnet | Optional |
| Logging out Users | Optional |
| Specifying a Mandatory Authentication Domain | Optional |

# Basic Portal Configuration

## Configuration Prerequisites

The portal feature provides a solution for user authentication and security authentication. However, the portal feature cannot implement this solution by itself. Currently, RADIUS authentication needs to be configured on the access device to cooperate with the portal feature to complete user authentication.

The prerequisites for portal authentication are as follows:

- The portal-enabled interfaces of the access device are configured with valid IP addresses or have obtained valid IP addresses through DHCP.
- The portal server and the RADIUS server have been installed and configured properly.
- With re-DHCP authentication, the invalid IP address check function of DHCP relay is enabled on the access device, and the DHCP server is installed and configured properly.
- With RADIUS authentication, usernames and passwords of the users are configured on the RADIUS server, and the RADIUS client configurations are performed on the access device. For information about RADIUS client configuration, refer to *AAA Configuration* in the *Security Volume*.
- To implement extended portal functions, you need install and configure the security policy server and ensure that the ACLs configured on the access device correspond to those specified for restricted resources and unrestricted resources on the security policy server respectively. For information about security policy server configuration, refer to *AAA Configuration* in the *Security Volume*.

---

**Note**

- For configuration about the security policy server, refer to *CAMS EAD Security Policy Component User Manual*.
- The ACL for restricted resources and that for unrestricted resources correspond to isolation ACL and security ACL on the security policy server respectively.
- You can modify the authorized ACL on the access device. However, the new ACL takes effect only for portal users logging on after the modification.

---

## Configuration Procedure

Basic Portal configurations include configuring the Portal server and enabling Portal on an interface. To configure a portal server, you need to specify the IP address of the portal server on the access device.

Follow these steps to perform basic portal configuration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a portal server | **portal server** *server-name* **ip** *ip-address* [ **key** *key-string* \| **port** *port-id* \| **url** *url-string* ] * | Required<br>By default, no portal server is configured. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable portal authentication on the interface | **portal server** *server-name* **method** { **direct** \| **layer3** \| **redhcp** } | Required<br>Disabled by default |

**Caution**

- Enabling portal authentication on a Layer 3 port is mutually exclusive with adding the port to an aggregation group.
- The destination port number that the device uses for sending packets to the portal server unsolicitedly must be the same as that the remote portal server actually uses.
- The portal server and its parameters can be deleted or modified only when the portal server is not referenced by any interface.
- The portal server to be referenced must exist.
- Only Layer 3 authentication mode can be used in applications with Layer 3 forwarding devices present between the authentication clients and the access device. However, Layer-3 authentication does not require any Layer-3 forwarding devices between the access device and the authentication clients.
- In re-DHCP authentication mode, a user is allowed to send packets using a public IP address before portal authentication, but the corresponding response packets are restricted.

## Configuring a Portal-Free Rule

A portal-free rule allows specified users to access specified external websites without portal authentication. Packets matching a portal-free rule will not trigger portal authentication and the users can directly access the specified external websites.

Follow these steps to configure a portal-free rule:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a portal-free rule | **portal free-rule** *rule-number* { **destination** { **any** \| **ip** { *ip-address* **mask** { *mask-length* \| *netmask* } \| **any** } } \| **source** { **any** \| [ **interface** *interface-type interface-number* \| **ip** { *ip-address* **mask** { *mask-length* \| *mask* } \| **any** } \| **mac** *mac-address* \| **vlan** *vlan-id* ] * } } * | Required |

**Note**

- If you specify both a VLAN and an interface in a portal-free rule, the interface must belong to the VLAN.
- You cannot configure two or more portal-free rules with the same filtering conditions. Otherwise, the system prompts that the rule already exists.
- No matter whether portal authentication is enabled, you can only add or remove a portal-free rule, rather than modifying it.

## Configuring an Authentication Subnet

By configuring authentication subnets, you specify that only packets from users on the authentication subnets trigger portal authentication. Packets that are neither from portal-free users nor from authentication subnets are discarded.

Follow these steps to configure an authentication subnet:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure an authentication subnet | **portal auth-network** *network-address* { *mask-length* \| *mask* } | Optional<br>By default, the authentication subnet is 0.0.0.0/0, which means that users with any source IP addresses are to be authenticated. |

**Note**

- Configuration of authentication subnets applies to only Layer 3 portal authentication.
- In direct authentication mode, the authentication subnet is 0.0.0.0/0.
- In re-DHCP authentication mode, the authentication subnet of an interface is the subnet to which the private IP address of the interface belongs.

## Logging out Users

Logging out a user terminates the authentication process for the user or removes the user.

Follow these steps to log out users:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Log out users | **portal delete-user** { *ip-address* \| **all** \| **interface** *interface-type interface-number* } | Required |

## Specifying a Mandatory Authentication Domain

After you specify a mandatory authentication domain for an interface, the device will use the mandatory authentication domain for authentication, authorization, and accounting (AAA) of the portal users on the interface, ignoring the domain names carried in the usernames. Thereby, you can specify different authentication domains for different interfaces as needed.

Follow these steps to specify an authentication domain for an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Specify an authentication domain for the interface | **portal domain** *domain-name* | Required<br>By default, no authentication domain is specified for an interface. |

**Note**

The device selects the authentication domain for a portal user on an interface in this order: the ISP domain specified for the interface, the ISP domain carried in the username, and the system default ISP domain. For descriptions on the default ISP domain, refer to *AAA Configuration* in the *Security Volume*.

## Displaying and Maintaining Portal

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the ACLs on a specified interface | **display portal acl** { **all** \| **dynamic** \| **static** } **interface** *interface-type interface-number* | Available in any view |
| Display portal connection statistics on a specified interface or all interfaces | **display portal connection statistics** { **all** \| **interface** *interface-type interface-number* } | Available in any view |
| Display information about a portal-free rule or all portal-free rules | **display portal free-rule** [ *rule-number* ] | Available in any view |
| Display the portal configuration of a specified interface | **display portal interface** *interface-type interface-number* | Available in any view |
| Display information about a specified portal server or all portal servers | **display portal server** [ *server-name* ] | Available in any view |
| Display portal server statistics on a specified interface or all interfaces | **display portal server statistics** { **all** \| **interface** *interface-type interface-number* } | Available in any view |
| Display TCP spoofing statistics | **display portal tcp-cheat statistics** | Available in any view |
| Display information about portal users on a specified interface or all interfaces | **display portal user** { **all** \| **interface** *interface-type interface-number* } | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear portal connection statistics on a specified interface or all interfaces | **reset portal connection statistics** {**all** \| **interface** *interface-type interface-number* } | Available in user view |
| Clear portal server statistics on a specified interface or all interfaces | **reset portal server statistics** { **all** \| **interface** *interface-type interface-number* } | Available in user view |
| Clear TCP spoofing statistics | **reset portal tcp-cheat statistics** | Available in user view |

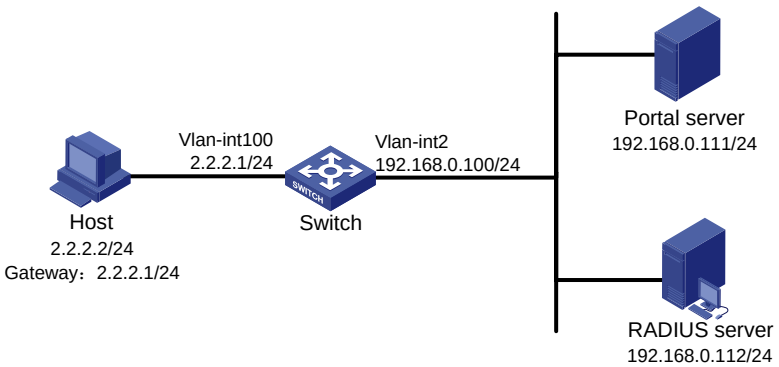
# Portal Configuration Examples

## Configuring Direct Portal Authentication

### Network requirements

- The host is directly connected to the switch and the switch is configured for direct authentication. The host is assigned with a public network IP address manually or automatically by a DHCP server. Before portal authentication, users using the host can access only the portal server. After passing portal authentication, they can access unrestricted Internet resources.
- A RADIUS server serves as the authentication/accounting server.

**Figure 1-4** Configure direct portal authentication




### Configuration procedure

**Note**

You need to configure IP addresses for the devices as shown in Figure 1-4 and ensure that routes are available between devices.

Configure the switch:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Set the server type to **extended**.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

# Specify that the ISP domain name should not be included in the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[Switch] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[Switch] domain default enable dm1
```

3) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt
- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

# Enable portal authentication on the interface connecting the host.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] ip address 2.2.2.1 255.255.255.0
[Switch–Vlan-interface100] portal server newpt method direct
[Switch] quit
```

# Configure the IP address of the interface connected with the portal server.

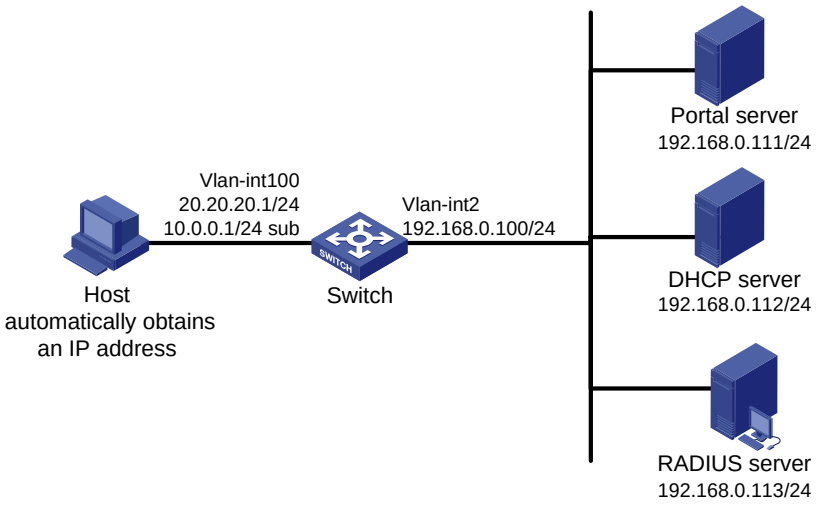
```
[Switch] interface vlan-interface 2
[Switch–Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch–Vlan-interface2] quit
```

# Configuring Re-DHCP Portal Authentication

## Network requirements

- The host is directly connected to the switch and the switch is configured for re-DHCP authentication. The host is assigned with an IP address through the DHCP server. Before portal authentication, the host uses an assigned private IP address. After passing portal authentication, it can get a public IP address and then users using the host can access unrestricted Internet resources.
- A RADIUS server serves as the authentication/accounting server.

**Figure 1-5** Configure re-DHCP portal authentication




## Configuration procedure

---

**Note**

- For re-DHCP authentication, you need to configure a public address pool (20.20.20.0/24, in this example) and a private address pool (10.0.0.0/24, in this example) on the DHCP server. The configuration steps are omitted. For DHCP configuration information, refer to *DHCP Configuration* in the *IP Services Volume*.
- For re-DHCP authentication, the switch must be configured as a DHCP relay agent (instead of a DHCP server) and the portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).
- You need to configure IP addresses for the devices as shown in Figure 1-5 and ensure that routes are available between devices.

---

Configure the switch:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Set the server type to **extended**.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.113
[Switch-radius-rs1] primary accounting 192.168.0.113
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

# Specify that the ISP domain name should not be included in the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[Switch] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[Switch] domain default enable dm1
```

3) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt
- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

# Configure the switch as a DHCP relay agent, and enable the invalid address check function.

```
[Switch] dhcp enable
[Switch] dhcp relay server-group 0 ip 192.168.0.112
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch–Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-select 0
[Switch-Vlan-interface100] dhcp relay address-check enable
```

# Enable re-DHCP portal authentication on the interface connecting the host.

```
[Switch–Vlan-interface100] portal server newpt method redhcp
[Switch–Vlan-interface100] quit
```

# Configure the IP address of the interface connected with the portal server.

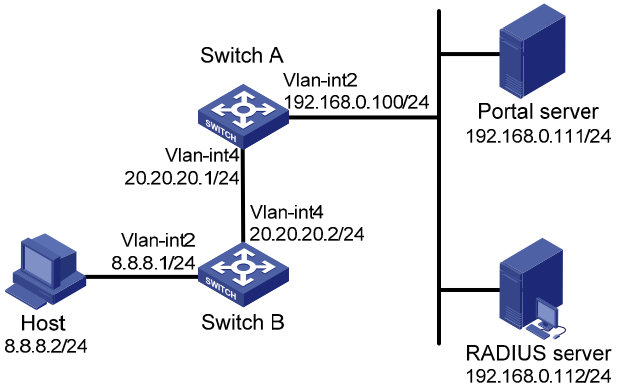
```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

## Configuring Layer 3 Portal Authentication

### Network requirements

- Switch A is configured for Layer 3 portal authentication. Before portal authentication, users can access only the portal server. After passing portal authentication, they can access unrestricted Internet resources.
- The host accesses Switch A through Switch B
- A RADIUS server serves as the authentication/accounting server.

**Figure 1-6** Configure Layer 3 portal authentication




### Configuration procedure

---

**Note**

You need to configure IP addresses for the devices as shown in Figure 1-6 and ensure that routes are available between devices..

---

Configure Switch A:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<SwitchA> system-view
[SwitchA] radius scheme rs1
```

# Set the server type to **extended**.

```
[SwitchA-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[SwitchA-radius-rs1] primary authentication 192.168.0.112
```

```
[SwitchA-radius-rs1] primary accounting 192.168.0.112
[SwitchA-radius-rs1] key authentication radius
[SwitchA-radius-rs1] key accounting radius
```

# Specify that the ISP domain name should not be included in the username sent to the RADIUS server.

```
[SwitchA-radius-rs1] user-name-format without-domain
[SwitchA-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[SwitchA] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[SwitchA] domain default enable dm1
```

3) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt
- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[SwitchA] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

# Enable portal authentication on the interface connecting Switch B.

```
[SwitchA] interface vlan-interface 4
[SwitchA–Vlan-interface4] ip address 20.20.20.1 255.255.255.0
[SwitchA–Vlan-interface4] portal server newpt method layer3
[SwitchA–Vlan-interface4] quit
```

# Configure the IP address of the interface connected with the portal server.

```
[SwitchA] interface vlan-interface 2
[SwitchA–Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[SwitchA–Vlan-interface2] quit
```

On Switch B, you need to configure a default route to subnet 192.168.0.0/24, setting the next hop as 20.20.20.1. The configuration steps are omitted.

## Configuring Direct Portal Authentication with Extended Functions

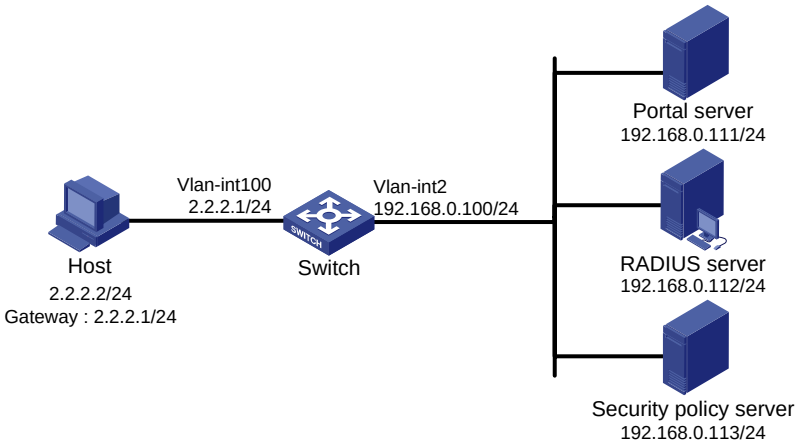
### Network requirements

- The host is directly connected to the switch and the switch is configured for direct extended portal authentication. The host is assigned with a public network IP address manually or automatically by a DHCP server. When users using the host have passed identity authentication but have not

passed security authentication, they can access only subnet 192.168.0.0/24. After passing security authentication, they can access unrestricted Internet resources.

- A RADIUS server serves as the authentication/accounting server.

**Figure 1-7** Configure direct portal authentication with extended functions




## Configuration procedure

**Note**

You need to configure IP addresses for the devices as shown in Figure 1-7 and ensure that routes are available between devices.

Configure the switch:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Set the server type to **extended**.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key accounting radius
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] user-name-format without-domain
```

# Configure the IP address of the security policy server.

```
[Switch-radius-rs1] security-policy-server 192.168.0.113
[Switch-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[Switch] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[Switch] domain default enable dm1
```

3) Configure the ACL (ACL 3000 ) for restricted resources and the ACL (ACL 3001) for unrestricted resources

---

**Note**

On the security policy server, you need to specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

---

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-adv-3000] quit
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

4) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt
- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

# Enable portal authentication on the interface connecting the host.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] ip address 2.2.2.1 255.255.255.0
[Switch–Vlan-interface100] portal server newpt method direct
[Switch] quit
```

# Configure the IP address of the interface connected with the portal server.

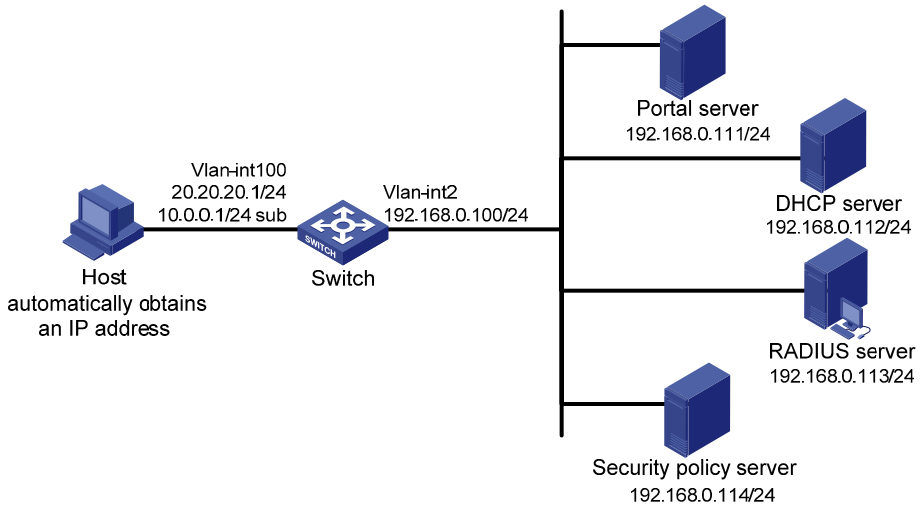
```
[Switch] interface vlan-interface 2
[Switch–Vlan-interface2] ip address 192.168.0.100 255.255.255.0
```

# Configuring Re-DHCP Portal Authentication with Extended Functions

## Network requirements

- The host is directly connected to the switch and the switch is configured for re-DHCP authentication. The host is assigned with an IP address through the DHCP server. Before portal authentication, the host uses an assigned private IP address. After passing portal authentication, it can get a public IP address.
- When users using the host have passed identity authentication but have not passed security authentication, they can access only subnet 192.168.0.0/24. After passing the security authentication, they can access unrestricted Internet resources.
- A RADIUS server serves as the authentication/accounting server.

**Figure 1-8** Configure re-DHCP portal authentication with extended functions




## Configuration procedure

---

**Note**

- For re-DHCP authentication, you need to configure a public address pool (20.20.20.0/24, in this example) and a private address pool (10.0.0.0/24, in this example) on the DHCP server. The configuration steps are omitted. For DHCP configuration information, refer to *DHCP Configuration* in the *IP Services Volume*.
- For re-DHCP authentication, the switch must be configured as a DHCP relay agent (instead of a DHCP server) and the portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).
- You need to configure IP addresses for the devices as shown in Figure 1-8 and ensure that routes are available between devices.

---

Configure the switch:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Set the server type to **extended**.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.113
[Switch-radius-rs1] primary accounting 192.168.0.113
[Switch-radius-rs1] key accounting radius
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] user-name-format without-domain
```

# Configure the IP address of the security policy server.

```
[Switch-radius-rs1] security-policy-server 192.168.0.114
[Switch-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[Switch] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[Switch] domain default enable dm1
```

3) Configure the ACL (ACL 3000 ) for restricted resources and the ACL (ACL 3001) for unrestricted resources

---

**Note**

On the security policy server, you need to specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

---

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-adv-3000] quit
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

4) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt

- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100
url http://192.168.0.111/portal
```

# Configure the switch as a DHCP relay agent, and enable the invalid address check function.

```
[Switch] dhcp enable
[Switch] dhcp relay server-group 0 ip 192.168.0.112
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch–Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-select 0
[Switch-Vlan-interface100] dhcp relay address-check enable
```

# Enable re-DHCP portal authentication on the interface connecting the host.

```
[Switch–Vlan-interface100] portal server newpt method redhcp
[Switch–Vlan-interface100] quit
```

# Configure the IP address of the interface connected with the portal server.

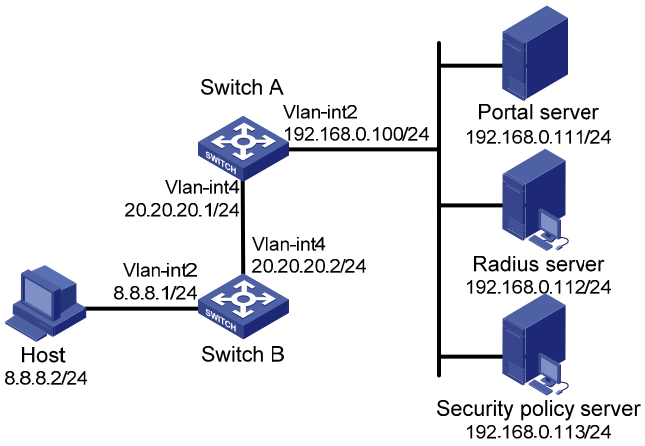
```
[Switch] interface vlan-interface 2
[Switch–Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch–Vlan-interface2] quit
```

## Configuring Layer 3 Portal Authentication with Extended Functions

### Network requirements

- Switch A is configured for Layer 3 extended portal authentication. When users have passed identity authentication but have not passed security authentication, they can access only subnet 192.168.0.0/24. After passing security authentication, they can access unrestricted Internet resources.
- The host accesses Switch A through Switch B.
- A RADIUS server serves as the authentication/accounting server.

**Figure 1-9** Configure Layer 3 portal authentication with extended functions



### Configuration procedure

**Note**

You need to configure IP addresses for the devices as shown in Figure 1-9 and ensure that routes are available between devices.

Configure Switch A:

1) Configure a RADIUS scheme

# Create a RADIUS scheme named **rs1** and enter its view.

```
<SwitchA> system-view
[SwitchA] radius scheme rs1
```

# Set the server type to **extended**.

```
[SwitchA-radius-rs1] server-type extended
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[SwitchA-radius-rs1] primary authentication 192.168.0.112
[SwitchA-radius-rs1] primary accounting 192.168.0.112
[SwitchA-radius-rs1] key accounting radius
[SwitchA-radius-rs1] key authentication radius
[SwitchA-radius-rs1] user-name-format without-domain
```

# Configure the IP address of the security policy server.

```
[SwitchA-radius-rs1] security-policy-server 192.168.0.113
[SwitchA-radius-rs1] quit
```

2) Configure an authentication domain

# Create an ISP domain named dm1 and enter its view.

```
[SwitchA] domain dm1
```

# Configure the ISP domain to use RADIUS scheme rs1.

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-isp-dm1] quit
```

# Configure dm1 as the default ISP domain, allowing all users to share the authentication and accounting methods of the default domain.

```
[SwitchA] domain default enable dm1
```

3) Configure the ACL (ACL 3000 ) for restricted resources and the ACL (ACL 3001) for unrestricted resources

**Note**

On the security policy server, you need to specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit ip
[SwitchA-acl-adv-3001] quit
```

4) Configure portal authentication

# Configure the portal server as follows:

- Name: newpt
- IP address: 192.168.0.111
- Key: portal
- Port number: 50100
- URL: http://192.168.0.111/portal.

```
[SwitchA] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

# Enable portal authentication on the interface connecting Switch B.

```
[SwitchA] interface vlan-interface 4
[SwitchA–Vlan-interface4] ip address 20.20.20.1 255.255.255.0
[SwitchA–Vlan-interface4] portal server newpt method layer3
[SwitchA–Vlan-interface4] quit
```

# Configure the IP address of the interface connected with the portal server.

```
[SwitchA] interface vlan-interface 2
[SwitchA–Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[SwitchA–Vlan-interface2] quit
```

On Switch B, you need to configure a default route to subnet 192.168.0.0/24, setting the next hop as 20.20.20.1. The configuration steps are omitted.

# Troubleshooting Portal

## Inconsistent Keys on the Access Device and the Portal Server

### Symptom

When a user is forced to access the portal server, the portal server displays neither the portal authentication page nor any error message. What the user sees is a blank web page.

### Analysis

The keys configured on the access device and the portal server are inconsistent, causing CHAP message exchange failure. As a result, the portal server does not display the authentication page.

### Solution

- Use the **display portal server** command to display the key for the portal server on the access device and view the key for the access device on the portal server.
- Use the **portal server** command to modify the key on the access device or modify the key for the access device on the portal server to ensure that the keys are consistent.

## Incorrect Server Port Number on the Access Device

### Symptom

After a user passes the portal authentication, you cannot force the user to log out by executing the **portal delete-user** command on the access device, but the user can log out by using the **disconnect** attribute on the authentication client.

### Analysis

When you execute the **portal delete-user** command on the access device to force the user to log out, the access device actively sends a REQ_LOGOUT message to the portal server. The default listening port of the portal server is 50100. However, if the listening port configured on the access device is not 50100, the destination port of the REQ_LOGOUT message is not the actual listening port on the server. Thus, the portal server cannot receive the REQ_LOGOUT message. As a result, you cannot force the user to log out the portal server.

When the user uses the **disconnect** attribute on the client to log out, the portal server actively sends a REQ_LOGOUT message to the access device. The source port is 50100 and the destination port of the ACK_LOGOUT message from the access device is the source port of the REQ_LOGOUT message so that the portal server can receive the ACK_LOGOUT message correctly, no matter whether the listening port is configured on the access device. Therefore, the user can log out the portal server.

### Solution

Use the **display portal server** command to display the listening port of the portal server on the access device and use the **portal server** command in the system view to modify it to ensure that it is the actual listening port of the portal server.

# Table of Contents

# 1 Port Security Configuration

When configuring port security, go to these sections for information you are interested in:



## Introduction to Port Security

### Port Security Overview

Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1X authentication and MAC authentication. It controls the access of unauthorized devices to the network by checking the source MAC address of an inbound frame and the access to unauthorized devices by checking the destination MAC address of an outbound frame.

With port security, you can define various port security modes to make a device learn only legal source MAC addresses, so that you can implement different network security management as needed. When a port security-enabled device detects an illegal frame, it triggers the corresponding port security feature and takes a pre-defined action automatically. This reduces your maintenance workload and greatly enhances system security.

The following types of frames are classified as illegal:

- Received frames with unknown source MAC addresses when MAC address learning is disabled.
- Received frames with unknown source MAC addresses when the number of MAC addresses learned by the port has already reached the upper limit.
- Frames from unauthenticated users.

---

**Note**

The security modes of the port security feature provide extended and combined use of 802.1X authentication and MAC authentication and therefore apply to scenarios that require both 802.1X authentication and MAC authentication. For scenarios that require only 802.1X authentication or MAC authentication for access control, however, you are recommended to configure the 802.1X authentication or MAC authentication for simplicity. For information about 802.1X and MAC authentication, refer to *802.1X Configuration* and *MAC Authentication Configuration* in the *Security Volume.*

---

## Port Security Features

### NTK

The need to know (NTK) feature checks the destination MAC addresses in outbound frames and allows frames to be sent to only devices passing authentication, thus preventing illegal devices from intercepting network traffic.

### Intrusion protection

The intrusion protection feature checks the source MAC addresses in inbound frames and takes a pre-defined action accordingly upon detecting illegal frames. The action may be disabling the port temporarily, disabling the port permanently, or blocking frames from the MAC address for three minutes (unmodifiable).

### Trap

The trap feature enables the device to send trap messages upon detecting specified frames that result from, for example, intrusion or user login/logout operations, helping you monitor special activities.

## Port Security Modes

Table 1-1 details the port security modes.

**Table 1-1** Port security modes

| Security mode | Description | Features |
|---|---|---|
| noRestrictions | Port security is disabled on the port and access to the port is not restricted. | In this mode, neither the NTK nor the intrusion protection feature is triggered. |
| autoLearn | In this mode, a port can learn a specified number of MAC addresses and save those addresses as secure MAC addresses. It permits only frames whose source MAC addresses are secure MAC addresses or static MAC addresses configured by using the **mac-address static** command.<br>When the number of secure MAC addresses reaches the upper limit, the port changes to work in secure mode. | In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal frame. |
| secure | In this mode, a port is disabled from learning MAC addresses and permits only frames whose source MAC addresses are secure MAC addresses or static MAC addresses configured by using the **mac-address static** command. | |
| userLogin | In this mode, a port performs 802.1X authentication of users in **portbased** mode.<br>A port in this mode can service multiple 802.1X users, but allows only one at a moment. | In this mode, neither NTK nor intrusion protection will be triggered. |

| Security mode | Description | Features |
|---|---|---|
| userLoginSecure | In this mode, a port performs 802.1X authentication of users in **portbased** mode and services only one user passing 802.1X authentication. | In any of these modes, the device will trigger NTK and intrusion protection upon detecting an illegal frame. |
| userLoginWithOUI | Similar to the userLoginSecure mode, a port in this mode performs 802.1X authentication of users and services only one user passing 802.1X authentication.<br>The port also permits frames from a user whose MAC address contains a specified OUI (organizationally unique identifier). | |
| macAddressWithRadius | In this mode, a port performs MAC authentication of users. | |
| macAddressOrUserLoginSecure | This mode is the combination of the userLoginSecure and macAddressWithRadius modes, with 802.1X authentication having a higher priority<br>The port performs MAC authentication upon receiving non-8021.x frames and performs 802.1X authentication upon receiving 802.1X frames. | |
| macAddressElseUserLoginSecure | This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority.<br>• Upon receiving a non-802.1X frame, a port in this mode performs only MAC authentication.<br>• Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication. | |
| userLoginSecureExt | In this mode, a port performs 802.1X authentication of users in macbased mode and supports multiple 802.1X users. | |
| macAddressOrUserLoginSecureExt | This mode is similar to the macAddressOrUserLoginSecure mode, except that it supports multiple 802.1X and MAC authentication users on the port. | |
| macAddressElseUserLoginSecureExt | This mode is similar to the macAddressElseUserLoginSecure mode, except that it supports multiple 802.1X and MAC authentication users on the port. | |

**Note**

- Currently, port security supports two authentication methods: 802.1X and MAC authentication. Different port security modes employ different authentication methods or different combinations of authentication methods.
- The maximum number of users a port supports is the lesser of the maximum number of secure MAC addresses or the maximum number of authenticated users the security mode supports. For example, in userLoginSecureExt mode, the maximum number of users a port supports is the lesser of the maximum number of secure MAC addresses configured or the maximum number of users that 802.1X supports.

**Tip**

These security mode naming rules may help you remember the modes:

- **userLogin** specifies port-based 802.1X authentication.
- **macAddress** specifies MAC address authentication.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, the protocol type of the authentication request determines whether to turn to the authentication method following the **Else**.
- In a security mode with **Or**, the protocol type of the authentication request determines which authentication method is to be used. However, 802.1X authentication is preferred by wireless users.
- **userLogin with Secure** specifies MAC-based 802.1X authentication.
- **Ext** indicates allowing multiple 802.1X users to be authenticated and get online. A security mode without **Ext** allows only one 802.1X user to be authenticated and get online.

# Port Security Configuration Task List

Complete the following tasks to configure port security:

| Task | | Remarks |
|---|---|---|
| Enabling Port Security | | Required |
| Setting the Maximum Number of Secure MAC Addresses | | Optional |
| Setting the Port Security Mode | | Required |
| Configuring Port Security Features | Configuring NTK | Optional |
| | Configuring Intrusion Protection | Choose one or more features as required. |
| | Configuring Trapping | |
| Configuring Secure MAC Addresses | | Optional |
| Ignoring Authorization Information from the Server | | Optional |

# Enabling Port Security

## Configuration Prerequisites

Before enabling port security, you need to disable 802.1X and MAC authentication globally.

## Configuration Procedure

Follow these steps to enable port security:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable port security | **port-security enable** | Required<br>Disabled by default |

Note that:

1) Enabling port security resets the following configurations on a port to the bracketed defaults. Then, values of these configurations cannot be changed manually; the system will adjust them based on the port security mode automatically:

- 802.1X (disabled), port access control method (macbased), and port access control mode (auto)
- MAC authentication (disabled)

2) Disabling port security resets the following configurations on a port to the bracketed defaults:

- Port security mode (noRestrictions)
- 802.1X (disabled), port access control method (macbased), and port access control mode (auto)
- MAC authentication (disabled)

3) Port security cannot be disabled if there is any user present on a port.

---

**Note**

- For detailed 802.1X configuration, refer to *802.1X Configuration* in the *Security Volume*.
- For detailed MAC-based authentication configuration, refer to *MAC Authentication Configuration* in the *Security Volume*.

---

# Setting the Maximum Number of Secure MAC Addresses

With port security enabled, more than one authenticated user is allowed on a port. The number of authenticated users allowed, however, cannot exceed the specified upper limit.

By setting the maximum number of secure MAC addresses allowed on a port, you can:

- Control the maximum number of users who are allowed to access the network through the port.
- Control the number of secure MAC addresses that can be added with port security.

Follow these steps to set the maximum number of secure MAC addresses allowed on a port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Set the maximum number of secure MAC addresses allowed on a port | **port-security max-mac-count** *count-value* | Required<br>Not limited by default |

**Note**

This configuration is different from that of the maximum number of MAC addresses that can be leaned by the port in MAC address management.

# Setting the Port Security Mode

## Configuration Prerequisites

Before setting the port security mode, ensure that:

- 802.1X is disabled, the port access control method is **macbased**, and the port access control mode is **auto**.
- MAC authentication is disabled.
- The port does not belong to any aggregation group.

The above requirements must be all met. Otherwise, you will see an error message and your configuration will fail. On the other hand, after setting the port security mode on a port, you cannot change any configurations of the first three requirements.

**Note**

- With port security disabled, you can configure the port security mode, but your configuration does not take effect.
- You cannot change the port security mode of a port when any user is present on the port.
- Before configuring the port to operate in autoLearn mode, set the maximum number of secure MAC addresses allowed on a port.

## Configuring Procedure

Follow these steps to enable any other port security mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set an OUI value for user authentication | **port-security oui** *oui-value* **index** *index-value* | Optional<br>Not configured by default.<br>The command is required for the **userlogin-withoui** mode. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Set the port security mode | **port-security port-mode** { **autolearn** \| **mac-authentication** \| **mac-else-userlogin-secure** \| **mac-else-userlogin-secure-ext** \| **secure** \| **userlogin** \| **userlogin-secure** \| **userlogin-secure-ext** \| **userlogin-secure-or-mac** \| **userlogin-secure-or-mac-ext** \| **userlogin-withoui** } | Required<br>By default, a port operates in noRestrictions mode. |

**Note**

- You cannot change the maximum number of secure MAC addresses allowed on a port that operates in autoLearn mode.
- OUI, defined by IEEE, is the first 24 bits of the MAC address and uniquely identifies a device vendor.
- You can configure multiple OUI values. However, a port in userLoginWithOUI mode allows only one 802.1X user and one user whose MAC address contains a specified OUI.
- After enabling port security, you can change the port security mode of a port only when the port is operating in noRestrictions mode, the default mode. To change the port security mode of a port operating in any other mode, use the **undo port-security port-mode** command to restore the default port security mode at first.
- You cannot change the port security mode of a port with users online.

# Configuring Port Security Features

## Configuring NTK

The need to know (NTK) feature checks the destination MAC addresses in outbound frames to allow frames to be forwarded to only devices passing authentication. The NTK feature supports three modes:

- **ntkonly**: Forwards only frames destined for authenticated MAC addresses.
- **ntk-withbroadcasts**: Forwards only frames destined for authenticated MAC addresses or the broadcast address.
- **ntk-withmulticasts**: Forwards only frames destined for authenticated MAC addresses, multicast addresses, or the broadcast address.

By default, NTK is disabled on a port and the port forwards all frames. With NTK configured, a port will discard any unicast packet with an unknown MAC address no matter in which mode it operates.

Follow these steps to configure the NTK feature:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure the NTK feature | **port-security ntk-mode** { **ntk-withbroadcasts** \| **ntk-withmulticasts** \| **ntkonly** } | Required<br>By default, NTK is disabled on a port and all frames are allowed to be sent. |

**Note**

Support for the NTK feature depends on the port security mode.

## Configuring Intrusion Protection

The intrusion protection enables a device to perform either of the following security policies when it detects illegal frames:

- **blockmac**: Adds the source MAC addresses of illegal frames to the blocked MAC addresses list and discards frames with blocked source MAC addresses. A blocked MAC address is restored to normal after being blocked for three minutes, which is fixed and cannot be changed.
- **disableport**: Disables the port permanently.
- **disableport-temporarily**: Disables the port for a specified period of time. Use the **port-security timer disableport** command to set the period.

Follow these steps to configure the intrusion protection feature:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure the intrusion protection feature | **port-security intrusion-mode** { **blockmac** \| **disableport** \| **disableport-temporarily** } | Required<br>By default, intrusion protection is disabled. |
| Return to system view | **quit** | — |
| Set the silence timeout during which a port remains disabled | **port-security timer disableport** *time-value* | Optional<br>20 seconds by default |

**Note**

On a port operating in either the macAddressElseUserLoginSecure mode or the macAddressElseUserLoginSecureExt mode, intrusion protection is triggered only after both MAC authentication and 802.1X authentication for the same frame fail.

### Configuring Trapping

The trapping feature enables a device to send trap information in response to four types of events:

- **addresslearned**: A port learns a new address.
- **dot1xlogfailure/dot1xlogon/dot1xlogoff**: A port learns 802.1X authentication failure/successful 802.1X authentication/802.1X user logoff.
- **ralmlogfailure**/**ralmlogoff**: A port learns MAC authentication failure/MAC authentication user logoff.
- **intrusion**: A port learns illegal frames.

Follow these steps to configure port security trapping:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable port security traps | **port-security trap** { **addresslearned** \| **dot1xlogfailure** \| **dot1xlogoff** \| **dot1xlogon** \| **intrusion** \| **ralmlogfailure** \| **ralmlogoff** \| **ralmlogon** } | Required<br>By default, no port security trap is enabled. |

## Configuring Secure MAC Addresses

Secure MAC addresses are special MAC addresses. They never age out or get lost if saved before the device restarts. One secure MAC address can be added to only one port in the same VLAN. Thus, you can bind a MAC address to one port in the same VLAN.

Secure MAC addresses can be:

- Learned by a port working in autoLearn mode.
- Manually configured through the command line interface (CLI) or management information base (MIB).

When the maximum number of secure MAC addresses is reached, no more can be added. The port allows only the packets with the source MAC address being the secure MAC address.

### Configuration Prerequisites

- Enable port security
- Set the maximum number of secure MAC addresses allowed on the port
- Set the port security mode to autoLearn

### Configuration Procedure

Follow these steps to configure a secure MAC address:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Configure a secure MAC address | In system view | **port-security mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* | Required<br>Use either approach<br>No secure MAC address is configured by default. |
| | In interface view | **interface** *interface-type interface-number* | |
| | | **port-security mac-address security** *mac-address* **vlan** *vlan-id* | |

**Note**

The configured secure MAC addresses are saved in the configuration file and will not get lost when the port goes up or goes down. After you save the configuration file, the secure MAC address saved in the configuration file are maintained even after the device restarts.

## Ignoring Authorization Information from the Server

After an 802.1X user or MAC authenticated user passes RADIUS authentication, the RADIUS server delivers the authorization information to the device. You can configure a port to ignore the authorization information from the RADIUS server.

Follow these steps to configure a port to ignore the authorization information from the RADIUS server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Ignore the authorization information from the RADIUS server | **port-security authorization ignore** | Required<br>By default, a port uses the authorization information from the RADIUS server. |

## Displaying and Maintaining Port Security

| To do… | Use the command… | Remarks |
|---|---|---|
| Display port security configuration information, operation information, and statistics about one or more ports or all ports | **display port-security** [ **interface** *interface-list* ] | Available in any view |
| Display information about secure MAC addresses | **display port-security mac-address security** [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] [ **count** ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about blocked MAC addresses | **display port-security mac-address block** [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] [ **count** ] | Available in any view |

# Port Security Configuration Examples

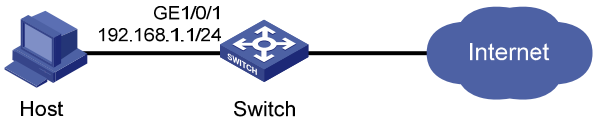
## Configuring the autoLearn Mode

### Network requirements

Restrict port GigabitEthernet 1/0/1 of the switch as follows:

- Allow up to 64 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as secure MAC addresses.
- After the number of secure MAC addresses reaches 64, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port is disabled and stays silence for 30 seconds.

**Figure 1-1** Network diagram for configuring the autoLearn mode




### Configuration procedure

1) Configure port security

# Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

# Enable intrusion protection trap.

```
[Switch] port-security trap intrusion
[Switch] interface gigabitethernet 1/0/1
```

# Set the maximum number of secure MAC addresses allowed on the port to 64.

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

# Set the port security mode to autoLearn.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

# Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-GigabitEthernet1/0/1] quit
[Switch] port-security timer disableport 30
```

2) Verify the configuration

After completing the above configurations, you can use the following command to view the port security configuration information:

```
<Switch> display port-security interface gigabitethernet 1/0/1
```

```
 Equipment port-security is enabled
 Intrusion trap is enabled
 Disableport Timeout: 30s
 OUI value:

GigabitEthernet1/0/1 is link-up
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePortTemporarily
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
```

As shown in the output, the maximum number of secure MAC addresses allowed on the port is 64, the port security mode is autoLearn, the intrusion protection trap is enabled, and the intrusion protection action is to disable the port (DisablePortTemporarily) for 30 seconds.

You can also use the above command repeatedly to track the number of MAC addresses learned by the port, or use the **display this** command in interface view to display the secure MAC addresses learned, as shown below:

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security intrusion-mode disableport-temporarily
 port-security mac-address security 0002-0000-0015 vlan 1
 port-security mac-address security 0002-0000-0014 vlan 1
 port-security mac-address security 0002-0000-0013 vlan 1
 port-security mac-address security 0002-0000-0012 vlan 1
 port-security mac-address security 0002-0000-0011 vlan 1
#
```

Issuing the **display port-security interface** command after the number of MAC addresses learned by the port reaches 64, you will see that the port security mode has changed to secure. When any frame with a new MAC address arrives, intrusion protection is triggered and you will see trap messages as follows:

```
#May  2 03:15:55:871 2000 Switch PORTSEC/1/VIOLATION:Traph3cSecureViolation
 A intrusion occurs!
 IfIndex: 9437207
 Port: 9437207
 MAC Addr: 0.2.0.0.0.21
 VLAN ID: 1
 IfAdminStatus: 1
```

In addition, you will see that the port security feature has disabled the port if you issue the following command:

```
[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 current state:  Port Security Disabled
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
......
```

The port should be re-enabled 30 seconds later.

```
[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
......
```

Now, if you manually delete several secure MAC addresses, the port security mode of the port will be restored to autoLearn, and the port will be able to learn MAC addresses again.

## Configuring the userLoginWithOUI Mode

### Network requirements

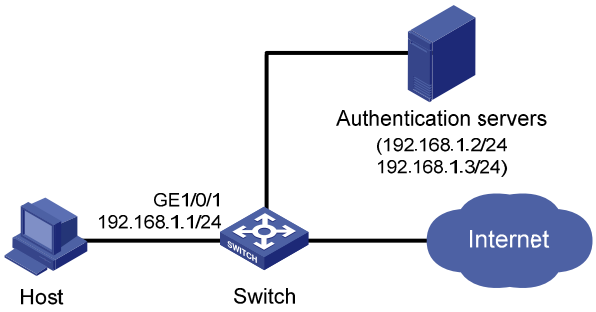
The client is connected to the switch through port GigabitEthernet 1/0/1. The switch authenticates the client by the RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

- RADIUS server 192.168.1.2 functions as the primary authentication server and the secondary accounting server, and RADIUS server 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is name, and that for accounting is money.
- All users belong to default domain sun, which can accommodate up to 30 users.
- The RADIUS server response timeout time is five seconds and the maximum number of RADIUS packet retransmission attempts is five. The switch sends real-time accounting packets to the RADIUS server at an interval of 15 minutes, and sends user names without domain names to the RADIUS server.

Restrict port GigabitEthernet 1/0/1 of the switch as follows:

- Allow only one 802.1X user to be authenticated.
- Allow up to 16 OUI values to be configured and allow one additional user whose MAC address has an OUI among the configured ones to access the port.

**Figure 1-2** Network diagram for configuring the userLoginWithOUI mode



### Configuration procedure

**Note**

- The following configuration steps cover some AAA/RADIUS configuration commands. For details about the commands, refer to *AAA Configuration* in the *Security Volume*.
- Configurations on the host and RADIUS servers are omitted.

1) Configure the RADIUS protocol

# Configure a RADIUS scheme named **radsun**.

```
<Switch> system-view
[Switch] radius scheme radsun
[Switch-radius-radsun] primary authentication 192.168.1.2
[Switch-radius-radsun] primary accounting 192.168.1.3
[Switch-radius-radsun] secondary authentication 192.168.1.3
[Switch-radius-radsun] secondary accounting 192.168.1.2
[Switch-radius-radsun] key authentication name
[Switch-radius-radsun] key accounting money
[Switch-radius-radsun] timer response-timeout 5
[Switch-radius-radsun] retry 5
[Switch-radius-radsun] timer realtime-accounting 15
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit
```

# Configure an ISP domain named **sun**.

```
[Switch] domain sun
[Switch-isp-sun] authentication default radius-scheme radsun
[Switch-isp-sun] authorization default radius-scheme radsun
[Switch-isp-sun] accounting default radius-scheme radsun
[Switch-isp-sun] access-limit enable 30
[Switch-isp-sun] quit
```

2) Configure port security

# Enable port security.

```
[Switch] port-security enable
```

# Add five OUI values.

```
[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2
[Switch] port-security oui 1234-0300-1111 index 3
[Switch] port-security oui 1234-0400-1111 index 4
[Switch] port-security oui 1234-0500-1111 index 5
[Switch] interface gigabitethernet 1/0/1
```

# Set the port security mode to userLoginWithOUI.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

3) Verify the configuration

After completing the above configurations, you can use the following command to view the configuration information of the RADIUS scheme named **radsun**:

```
<Switch> display radius scheme radsun
SchemeName  : radsun
  Index : 1                            Type : standard
  Primary Auth IP  : 192.168.1.2      Port : 1812   State : active
  Primary Acct IP  : 192.168.1.3      Port : 1813   State : active
  Second  Auth IP  : 192.168.1.3      Port : 1812   State : active
  Second  Acct IP  : 192.168.1.2      Port :1813    State : active
  Auth Server Encryption Key : name
  Acct Server Encryption Key : money
  Accounting-On packet disable, send times : 5 , interval : 3s
  Interval for timeout(second)                              : 5
  Retransmission times for timeout                          : 5
  Interval for realtime accounting(minute)                  : 15
  Retransmission times of realtime-accounting packet        : 5
  Retransmission times of stop-accounting packet            : 500
  Quiet-interval(min)                                       : 5
  Username format                                           : without-domain
  Data flow unit                                            : Byte
  Packet unit                                               : one
```

Use the following command to view the configuration information of the ISP domain named **sun**:

```
<Switch> display domain sun
   Domain = sun
   State = Active
   Access-limit = 30
   Accounting method = Required
   Default authentication scheme      : radius=radsun
   Default authorization scheme       : radius=radsun
   Default accounting scheme          : radius=radsun
   Domain User Template:
   Idle-cut = Disabled
   Self-service = Disabled
```

Use the following command to view the port security configuration information:

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 123401
   Index is 2,  OUI value is 123402
   Index is 3,  OUI value is 123403
   Index is 4,  OUI value is 123404
   Index is 5,  OUI value is 123405

 GigabitEthernet1/0/1 is link-up
   Port mode is userLoginWithOUI
```

```
  NeedToKnow mode is disabled
  Intrusion Protection mode is NoAction
  Max MAC address number is not configured
  Stored MAC address number is 0
  Authorization is permitted
```

After an 802.1X user gets online, you can see that the number of secure MAC addresses stored is 1. You can also use the following command to view information about 802.1X users:

```
<Switch> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 EAD quick deploy is disabled

  Configuration: Transmit Period   30 s,  Handshake Period       15 s
                 Quiet Period      60 s,  Quiet Period Timer is disabled
                 Supp Timeout      30 s,  Server Timeout        100 s
                 The maximal retransmitting times    2
  EAD quick deploy configuration:
               EAD timeout:    30m

 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Handshake is enabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   Guest VLAN: 0
   Max number of on-line users is 256

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

In addition, the port allows an additional user whose MAC address has an OUI among the specified OUIs to access the port. You can use the following command to view the related information:

```
<Switch> display mac-address interface gigabitethernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
```

```
1234-0300-0011  1         Learned        GigabitEthernet1/0/1    AGING

  ---  1 mac address(es) found  ---
```

## Configuring the macAddressElseUserLoginSecure Mode

### Network requirements

The client is connected to the switch through GigabitEthernet 1/0/1. The switch authenticates the client by the RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

Restrict port GigabitEthernet 1/0/1 of the switch as follows:

- Allow more than one MAC authenticated user to log on.
- For 802.1X users, perform MAC authentication first and then, if MAC authentication fails, 802.1X authentication. Allow only one 802.1X user to log on.
- Set fixed username and password for MAC-based authentication. Set the total number of MAC authenticated users and 802.1X-authenticated users to 64.
- Enable NTK to prevent frames from being sent to unknown MAC addresses.

See Figure 1-2.

### Configuration procedure

---

**Note**

- Configurations on the host and RADIUS servers are omitted.

---

1) Configure the RADIUS protocol

The required RADIUS authentication/accounting configurations are the same as those in Configuring the userLoginWithOUI Mode.

2) Configure port security

# Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

# Configure a MAC authentication user, setting the user name and password to aaa and 123456 respectively.

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
[Switch] interface gigabitethernet 1/0/1
```

# Set the maximum number of secure MAC addresses allowed on the port to 64.

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

# Set the port security mode to macAddressElseUserLoginSecure.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

# Set the NTK mode of the port to ntkonly.

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

3) Verify the configuration

After completing the above configurations, you can use the following command to view the port security configuration information:

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:

 GigabitEthernet1/0/1 is link-up
   Port mode is macAddressElseUserLoginSecure
   NeedToKnow mode is NeedToKnowOnly
   Intrusion Protection mode is NoAction
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
```

Use the following command to view MAC authentication information:

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 3, failed: 7
  Current online user number is 3
    MAC ADDR         Authenticate state           AuthIndex
    1234-0300-0011   MAC_AUTHENTICATOR_SUCCESS     13
    1234-0300-0012   MAC_AUTHENTICATOR_SUCCESS     14
    1234-0300-0013   MAC_AUTHENTICATOR_SUCCESS     15
```

Use the following command to view 802.1X authentication information:

```
<Switch> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:    30m

 Total maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Handshake is enabled
   The port is an authenticator
```

```
  Authentication Mode is Auto
  Port Control Type is Mac-based
  Guest VLAN: 0
  Max number of on-line users is 256

  EAPOL Packet: Tx 16331, Rx 102
  Sent EAP Request/Identity Packets : 16316
       EAP Request/Challenge Packets: 6
       EAP Success Packets: 4, Fail Packets: 5
  Received EAPOL Start Packets : 6
           EAPOL LogOff Packets: 2
           EAP Response/Identity Packets : 80
           EAP Response/Challenge Packets: 6
           Error Packets: 0
1. Authenticated user : MAC address: 0002-0000-0011

  Controlled User(s) amount to 1
```

In addition, as NTK is enabled, frames with unknown destination MAC addresses, multicast addresses, and broadcast addresses should be discarded.

# Troubleshooting Port Security

## Cannot Set the Port Security Mode

### Symptom

Cannot set the port security mode.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
 Error:When we change port-mode, we should first change it to noRestrictions, then change it to the other.
```

### Analysis

For a port working in a port security mode other than noRestrictions, you cannot change the port security mode by using the **port-security port-mode** command directly.

### Solution

Set the port security mode to noRestrictions first.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

## Cannot Configure Secure MAC Addresses

### Symptom

Cannot configure secure MAC addresses.

```
[Switch-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
 Error:Can not operate security MAC address for current port mode is not autoLearn!
```

### Analysis

No secure MAC address can be configured on a port operating in a port security mode other than autoLearn.

### Solution

Set the port security mode to autoLearn.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
[Switch-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

## Cannot Change Port Security Mode When a User Is Online

### Symptom

Port security mode cannot be changed when an 802.1X-authenticated or MAC authenticated user is online.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
 Error:Cannot configure port-security for there is 802.1X user(s) on line on port GigabitEthernet1/0/1.
```

### Analysis

Changing port security mode is not allowed when an 802.1X-authenticated or MAC authenticated user is online.

### Solution

Use the **cut** command to forcibly disconnect the user from the port before changing the port security mode.

```
[Switch-GigabitEthernet1/0/1] quit
[Switch] cut connection interface gigabitethernet 1/0/1
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
```

# Table of Contents

# 1 IP Source Guard Configuration

When configuring IP Source Guard, go to these sections for information you are interested in:



## IP Source Guard Overview

By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a match, the port forwards the packet. Otherwise, the port discards the packet.

IP source guard filters packets based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry
- IP-VLAN-port binding entry
- MAC-VLAN-port binding entry
- IP-MAC-VLAN-port binding entry

You can manually set static binding entries, or use DHCP snooping or DHCP relay to provide dynamic binding entries. Binding is on a per-port basis. After a binding entry is configured on a port, it is effective only to the port.

**Caution**

Enabling IP source guard on a port is mutually exclusive with adding the port to an aggregation group.

## Configuring a Static Binding Entry

Follow these steps to configure a static binding entry:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure a static binding entry | **user-bind** { **ip-address** *ip-address* \| **ip-address** *ip-address* **mac-address** *mac-address* \| **mac-address** *mac-address* } [ **vlan** *vlan-id* ] | Required<br>No static binding entry exists by default. |

**Note**

- The system does not support repeatedly binding a binding entry to one port.
- For products supporting multi-port binding, a binding entry can be configured to multiple ports; for products that do not support multi-port binding, a binding entry can be configured to only one port.
- Supported binding entry types vary by device.
- In a valid binding entry, the MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address, and the IP address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.
- A static binding entry can be configured on only Layer-2 Ethernet ports.

## Configuring Dynamic Binding Function

After the dynamic binding function is enabled on a port, IP source guard will receive and process corresponding DHCP snooping or DHCP relay entries, which contain such information as MAC address, IP address, VLAN tag, port information or entry type. It adds the obtained information to the dynamic binding entries to enable the port to filter packets according to the binding entries.

Follow these steps to configure port filtering:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Configure dynamic binding function | **ip check source** { **ip-address** \| **ip-address mac-address** \| **mac-address** } | Required<br>Not configured by default |

**Note**

- The dynamic binding function can be configured on Layer-2 Ethernet ports and VLAN interfaces.
- A port takes only the latest dynamic binding entries configured on it.

# Displaying and Maintaining IP Source Guard

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about static binding entries | **display user-bind** [ **interface** *interface-type interface-number* \| **ip-address** *ip-address* \| **mac-address** *mac-address* ] | Available in any view |
| Display information about dynamic binding entries | **display ip check source** [ **interface** *interface-type interface-number* \| **ip-address** *ip-address* \| **mac-address** *mac-address* ] | Available in any view |

# IP Source Guard Configuration Examples

## Static Binding Entry Configuration Example

### Network requirements

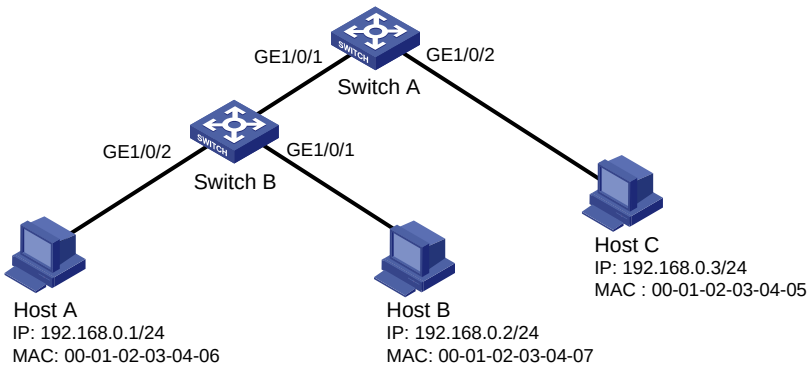
As shown in Figure 1-1, Host A and Host B are connected to ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/1 of Switch B respectively, Host C is connected to port GigabitEthernet 1/0/2 of Switch A, and Switch B is connected to port GigabitEthernet 1/0/1 of Switch A.

Configure static binding entries on Switch A and Switch B to meet the following requirements:

- On port GigabitEthernet 1/0/2 of Switch A, only IP packets from Host C can pass.
- On port GigabitEthernet 1/0/1 of Switch A, only IP packets from Host A can pass.
- On port GigabitEthernet 1/0/2 of Switch B, only IP packets from Host A can pass.
- On port GigabitEthernet 1/0/1 of Switch B, only IP packets from Host B can pass.

### Network diagram

**Figure 1-1** Network diagram for configuring static binding entries




### Configuration procedure

1) Configure Switch A

# Configure the IP addresses of various interfaces (omitted).

# Configure port GigabitEthernet 1/0/2 of Switch A to allow only IP packets with the source MAC address of 00-01-02-03-04-05 and the source IP address of 192.168.0.3 to pass.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.3 mac-address 0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

# Configure port GigabitEthernet 1/0/1 of Switch A to allow only IP packets with the source MAC address of 00-01-02-03-04-06 and the source IP address of 192.168.0.1 to pass.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

2) Configure Switch B

# Configure the IP addresses of various interfaces (omitted).

# Configure port GigabitEthernet 1/0/2 of Switch B to allow only IP packets with the source MAC address of 00-01-02-03-04-06 and the source IP address of 192.168.0.1 to pass.

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
[SwitchB-GigabitEthernet1/0/2] quit
```

# Configure port GigabitEthernet 1/0/1 of Switch B to allow only IP packets with the source MAC address of 00-01-02-03-04-07 and the source IP address of 192.168.0.2 to pass.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.2 mac-address 0001-0203-0407
```

3) Verify the configuration

# On Switch A, static binding entries are configured successfully.

```
<SwitchA> display user-bind
Total entries found: 2
 MAC               IP              Vlan   Port                         Status
 0001-0203-0405   192.168.0.3      N/A    GigabitEthernet1/0/2         Static
 0001-0203-0406   192.168.0.1      N/A    GigabitEthernet1/0/1         Static
```

# On Switch B, static binding entries are configured successfully.

```
<SwitchB> display user-bind
Total entries found: 2
MAC               IP              Vlan   Port                         Status
 0001-0203-0406   192.168.0.1      N/A    GigabitEthernet1/0/2         Static
 0001-0203-0407   192.168.0.2      N/A    GigabitEthernet1/0/1         Static
```

## Dynamic Binding Function Configuration Example

### Network requirements

Switch A connects to Client A and the DHCP server through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively. DHCP snooping is enabled on Switch A.

Detailed requirements are as follows:

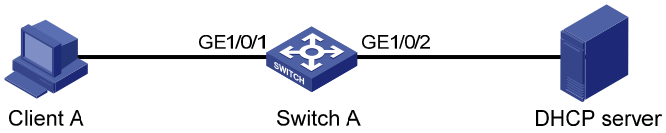
- Client A (with the MAC address of 00-01-02-03-04-06) obtains an IP address through the DHCP server.
- On Switch A, create a DHCP snooping entry for Client A.
- On port GigabitEthernet 1/0/1 of Switch A, enable dynamic binding function to prevent attackers from using forged IP addresses to attack the server.

**Note**

For detailed configuration of a DHCP server, refer to *DHCP Configuration* in the *IP Service Volume.*

## Network diagram

**Figure 1-2** Network diagram for configuring dynamic binding function




## Configuration procedure

1) Configure Switch A

# Configure dynamic binding function on port GigabitEthernet 1/0/1.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet1/0/1
[SwitchA-GigabitEthernet1/0/1] ip check source ip-address mac-address
[SwitchA-GigabitEthernet1/0/1] quit
```

# Enable DHCP snooping.

```
[SwitchA] dhcp-snooping
```

# Configure the port connecting to the DHCP server as a trusted port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/2] quit
```

2) Verify the configuration

# Display dynamic binding function is configured successfully on port GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 ip check source ip-address mac-address
#
return
```

# Display the dynamic binding entries that port GigabitEthernet 1/0/1 has obtained from DHCP snooping.

```
[SwitchA-GigabitEthernet1/0/1] display ip check source
Total entries found: 1
 MAC               IP              Vlan   Port                        Status
 0001-0203-0406    192.168.0.1     1      GigabitEthernet 1/0/1        DHCP-SNP
```

# Display the dynamic entries of DHCP snooping and check it is identical with the dynamic entries that port GigabitEthernet 1/0/1 has obtained.

```
[SwitchA-GigabitEthernet1/0/1] display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type IP Address      MAC Address    Lease        VLAN Interface
==== =============== ============== ============ ==== =================
D    192.168.0.1     0001-0203-0406 86335        1    GigabitEthernet1/0/1
```

As you see, port GigabitEthernet 1/0/1 has obtained the dynamic entries generated by DHCP snooping after it is configured with dynamic binding function.

# Troubleshooting IP Source Guard

## Failed to Configure Static Binding Entries and Dynamic Binding Function

### Symptom

Configuring static binding entries and dynamic binding function fails on a port.

### Analysis

IP Source Guard is not supported on the port which has joined an aggregation group. Neither static binding entries nor dynamic binding function can be configured on the port which has joined an aggregation group.

### Solution

Remove the port from the aggregation group.

# Table of Contents

# 1 SSH2.0 Configuration

When configuring SSH2.0, go to these sections for information you are interested in:



## SSH2.0 Overview

### Introduction to SSH2.0

Secure Shell (SSH) offers an approach to securely logging into a remote device. By encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception.

The device can not only work as an SSH server to support connections with SSH clients, but also work as an SSH client to allow users to establish SSH connections with a remote device acting as the SSH server.

**Note**

Currently, when acting as an SSH server, the device supports two SSH versions: SSH2.0 and SSH1. When acting as an SSH client, the device supports SSH2.0 only.

### Operation of SSH

The session establishment and interaction between an SSH client and the SSH server involves the following five stages:

**Table 1-1** Stages in session establishment and interaction between an SSH client and the server

| Stages | Description |
|---|---|
| Version negotiation | SSH1 and SSH2.0 are supported. The two parties negotiate a version to use. |
| Key and algorithm negotiation | SSH supports multiple algorithms. The two parties negotiate an algorithm for communication. |
| Authentication | The SSH server authenticates the client in response to the client's authentication request. |

| Stages | Description |
| --- | --- |
| Session request | After passing authentication, the client sends a session request to the server. |
| Interaction | After the server grants the request, the client and server start to communicate with each other. |

### Version negotiation

1) The server opens port 22 to listen to connection requests from clients.
2) The client sends a TCP connection request to the server. After the TCP connection is established, the server sends the first packet to the client, which includes a version identification string in the format of “SSH-<primary protocol version number>.<secondary protocol version number>-<software version number>”. The primary and secondary protocol version numbers constitute the protocol version number, while the software version number is used for debugging.
3) The client receives and resolves the packet. If the protocol version of the server is lower but supportable, the client uses the protocol version of the server; otherwise, the client uses its own protocol version.
4) The client sends to the server a packet that contains the number of the protocol version it decides to use. The server compares the version carried in the packet with that of its own. If the server supports the version, the server and client will use the version. Otherwise, the negotiation fails.
5) If the negotiation is successful, the server and the client proceed with key and algorithm negotiation; otherwise, the server breaks the TCP connection.

**Note**

All the packets involved in the above steps are transferred in plain text.

### Key and algorithm negotiation

- The server and the client send key algorithm negotiation packets to each other, which include the supported public key algorithm list, encryption algorithm list, Message Authentication Code (MAC) algorithm list, and compression algorithm list.
- Based on the received algorithm negotiation packets, the server and the client figure out the algorithms to be used. If the negotiation of any type of algorithm fails, the algorithm negotiation fails and the server tears down the connection with the client.
- The server and the client use the DH key exchange algorithm and parameters such as the host key pair to generate the session key and session ID and the client authenticates the identity of the server.

Through the above steps, the server and client get the same session key and session ID. The session key will be used to encrypt and decrypt data exchanged between the server and client later, and the session ID will be used to identify the session established between the server and client and will be used in the authentication stage.

**Caution**

Before the negotiation, the server must have already generated a DSA or RSA key pair, which is not only used for generating the session key, but also used by the client to authenticate the identity of the server. For details about DSA and RSA key pairs, refer to *Public Key Configuration* in the *Security Volume*.

## Authentication

SSH provides two authentication methods: password authentication and publickey authentication.

- Password authentication: The server uses AAA for authentication of the client. During password authentication, the client encrypts its username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the server decrypts the username and password, checks the validity of the username and password locally or by a remote AAA server, and then informs the client of the authentication result**.**
- Publickey authentication: The server authenticates the client by the digital signature. During publickey authentication, the client sends to the server a publickey authentication request that contains its username, public key, and publickey algorithm information. The server checks whether the public key is valid. If the public key is invalid, the authentication fails; otherwise, the server authenticates the client by the digital signature. Finally, the server sends a message to the client to inform the success or failure of the authentication. Currently, the device supports two publickey algorithms for digital signature: RSA and DSA.

The following gives the steps of the authentication stage:

1) The client sends to the server an authentication request, which includes the username, authentication method (password authentication or publickey authentication), and information related to the authentication method (for example, the password in the case of password authentication).
2) The server authenticates the client. If the authentication fails, the server informs the client by sending a message, which includes a list of available methods for re-authentication.
3) The client selects a method from the list to initiate another authentication.
4) The above process repeats until the authentication succeeds or the failed authentication times exceed the maximum of authentication attempts and the session is torn down.

**Note**

Besides password authentication and publickey authentication, SSH2.0 provides another two authentication methods:

- **password-publickey**: Performs both password authentication and publickey authentication if the client is using SSH2.0 and performs either if the client is running SSH1.
- **any**: Performs either password authentication or publickey authentication.

### Session request

After passing authentication, the client sends a session request to the server, while the server listens to and processes the request from the client. After successfully processing the request, the server sends back to the client an SSH_SMSG_SUCCESS packet and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an SSH_SMSG_FAILURE packet, indicating that the processing fails or it cannot resolve the request.

### Interaction

In this stage, the server and the client exchanges data in the following way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

---

**Note**

- In the interaction stage, you can execute commands from the client by pasting the commands in text format (the text must be within 2000 bytes). It is recommended that the commands are in the same view; otherwise, the server may not be able to perform the commands correctly.
- If the command text exceeds 2000 bytes, you can execute the commands by saving the text as a configuration file, uploading the configuration file to the server through SFTP, and then using the configuration file to restart the server.

---

# Configuring the Device as an SSH Server

## SSH Server Configuration Task List

Complete the following tasks to configure an SSH server:

| Task | Remarks |
|---|---|
| Generating a DSA or RSA Key Pair | Required |
| Enabling SSH Server | Required |
| Configuring the User Interfaces for SSH Clients | Required |
| Configuring a Client Public Key | Required for publickey authentication users and optional for password authentication users |
| Configuring an SSH User | Optional |
| Setting the SSH Management Parameters | Optional |

## Generating a DSA or RSA Key Pair

The DSA or RSA key pair will be used to generate the session ID in the key and algorithm negotiation stage and used by the client to authenticate the server.

Follow these steps to generate a DSA or RSA key pair on the SSH server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Generate the local DSA or RSA key pair | **public-key local create** { **dsa** \| **rsa** } | Required<br>By default, there is neither DSA key pair nor RSA key pair. |

**Note**

- For details about the **public-key local create** command, refer to *Public Key Commands* in the *Security Volume*.
- To ensure that all SSH clients can log into the SSH server successfully, you are recommended to generate both DSA and RSA key pairs on the SSH server. This is because different SSH clients may use different publickey algorithms, though a single client usually uses only one type of publickey algorithm.
- The **public-key local create rsa** command generates two RSA key pairs: a server key pair and a host key pair. Each of the key pairs consists of a public key and a private key. The public key in the server key pair of the SSH server is used in SSH1 to encrypt the session key for secure transmission of the key. As SSH2 uses the DH algorithm to generate the session key on the SSH server and client respectively, no session key transmission is required in SSH2 and the server key pair is not used.
- The length of the modulus of RSA server keys and host keys must be in the range 512 to 2048 bits. Some SSH2 clients require that the length of the key modulus be at least 768 bits on the SSH server side.
- The **public-key local create dsa** command generates only the host key pair. SSH1 does not support the DSA algorithm.
- The length of the modulus of DSA host keys must be in the range 512 to 2048 bits. Some SSH2 clients require that the length of the key modulus be at least 768 bits on the SSH server side.

## Enabling SSH Server

Follow these steps to enable SSH server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the SSH server function | **ssh server enable** | Required<br>Disabled by default |

## Configuring the User Interfaces for SSH Clients

An SSH client accesses the device through a VTY user interface. Therefore, you need to configure the user interfaces for SSH clients to allow SSH login. Note that the configuration takes effect only for clients logging in after the configuration.

Follow these steps to configure the protocols for the current user interface to support:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter user interface view of one or more user interfaces | **user-interface vty** *number* [ *ending-number* ] | — |
| Set the login authentication mode to **scheme** | **authentication-mode scheme** [ **command-authorization** ] | Required<br>By default, the authentication mode is **password**. |
| Configure the user interface(s) to support SSH login | **protocol inbound** { **all** \| **ssh** } | Optional<br>All protocols are supported by default. |

**Caution**

- For detailed information about the **authentication-mode** and **protocol inbound** commands, refer to *User Interface Commands* of the *System Volume.*
- If you configure a user interface to support SSH, be sure to configure the corresponding authentication method with the **authentication-mode scheme** command.
- For a user interface configured to support SSH, you cannot change the authentication mode. To change the authentication mode, undo the SSH support configuration first.

## Configuring a Client Public Key

**Note**

This configuration task is only necessary for SSH users using publickey authentication.

For each SSH user that uses publickey authentication to login, you must configure the client's DSA or RSA host public key on the server, and configure the client to use the corresponding private key.

To configure the public key of an SSH client, you can:

- Configure it manually: You can input or copy the public key to the local host. The copied public key must have not been converted and be in the distinguished encoding rules (DER) encoding format.
- Import it from the public key file: During the import process, the system will automatically convert the public key to a string coded using the Public Key Cryptography Standards (PKCS). Before importing the public key, you must upload the public key file (in binary) to the local host through FTP or TFTP.

**Caution**

- You are recommended to configure a client public key by importing it from a public key file.
- You can configure at most 20 client pubic keys on an SSH server.

### Configuring a client public key manually

Follow these steps to configure the client public key manually:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter public key view | **public-key peer** *keyname* | — |
| Enter public key code view | **public-key-code begin** | — |
| Configure a client public key | Enter the content of the public key | Required<br>Spaces and carriage returns are allowed between characters. |
| Return from public key code view to public key view | **public-key-code end** | —<br>When you exit public key code view, the system automatically saves the public key. |
| Return from public key view to system view | **peer-public-key end** | — |

### Importing a client public key from a public key file

Follow these steps to import a public key from a public key file:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Import the public key from a public key file | **public-key peer** *keyname*<br>**import sshkey** *filename* | Required |

**Note**

For information about client side public key configuration and the relevant commands, refer to *Public Key Configuration* in the *Security Volume*.

## Configuring an SSH User

This configuration allows you to create an SSH user and specify the service type and authentication mode.

Follow these steps to configure an SSH user and specify the service type and authentication mode:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create an SSH user, and specify the service type and authentication mode | For Stelnet users | **ssh user** *username* **service-type stelnet authentication-type** { **password** \| { **any** \| **password-publickey** \| **publickey** } **assign publickey** *keyname* } | Required<br>Use either command. |
| | For all users or SFTP users | **ssh user** *username* **service-type** { **all** \| **sftp** } **authentication-type** { **password** \| { **any** \| **password-publickey** \| **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* } | |

**Caution**

- A user without an SSH account can still pass password authentication and log into the server through Stelnet or SFTP, as long as the user can pass AAA authentication and the service type is SSH.
- An SSH server supports up to 1024 SSH users.
- The service type of an SSH user can be Stelnet (Secure Telnet) or SFTP (Secure FTP). For information about Stelnet, refer to SSH2.0 Overview. For information about SFTP, refer to SFTP Overview.
- For successful login through SFTP, you must set the user service type to **sftp** or **all**.
- As SSH1 does not support service type **sftp**, if the client uses SSH1 to log into the server, you must set the service type to **stelnet** or **all** on the server. Otherwise, the client will fail to log in.
- The working folder of an SFTP user is subject to the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.
- The configured authentication method takes effect only for users logging in after the configuration.

**Note**

For users using publickey authentication:

- You must configure on the device the corresponding username and public keys.
- After login, the commands available for a user are determined by the user privilege level, which is configured with the **user privilege level** command on the user interface.

For users using password authentication:

- You can configure the accounting information either on the device or on the remote authentication server (such as RADIUS authentication server).
- After login, the commands available to a user are determined by AAA authorization.

## Setting the SSH Management Parameters

SSH management includes:

- Enabling the SSH server to be compatible with SSH1 client
- Setting the server key pair update interval, applicable to users using SSH1 client
- Setting the SSH user authentication timeout period
- Setting the maximum number of SSH authentication attempts

Setting the above parameters can help avoid malicious guess at and cracking of the keys and usernames, securing your SSH connections.

Follow these steps to set the SSH management parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the SSH server to work with SSH1 clients | **ssh server compatible-ssh1x enable** | Optional<br>By default, the SSH server can work with SSH1 clients. |
| Set the RSA server key pair update interval | **ssh server rekey-interval** *hours* | Optional<br>0 by default, that is, the RSA server key pair is not updated. |
| Set the SSH user authentication timeout period | **ssh server authentication-timeout** *time-out-value* | Optional<br>60 seconds by default |
| Set the maximum number of SSH authentication attempts | **ssh server authentication-retries** *times* | Optional<br>3 by default |

**Note**

Authentication will fail if the number of authentication attempts (including both publickey and password authentication) exceeds that specified in the **ssh server authentication-retries** command.

# Configuring the Device as an SSH Client

## SSH Client Configuration Task List

Complete the following tasks to configure an SSH client:

| Task | Remarks |
|---|---|
| Specifying a Source IP address/Interface for the SSH client | Optional |
| Configuring Whether First-time Authentication is Supported | Optional |
| Establishing a Connection Between the SSH Client and the Server | Required |

## Specifying a Source IP address/Interface for the SSH client

This configuration task allows you to specify a source IP address or interface for the client to access the SSH server, improving service manageability.

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Specify a source IP address or interface for the SSH client | Specify a source IPv4 address or interface for the SSH client | **ssh client source** { **ip** *ip-address* \| **interface** *interface-type interface-number* } | Required<br>By default, the address of the interface decided by the routing is used to access the SSH server |
| | Specify a source IPv6 address or interface for the SSH client | **ssh client ipv6 source** { **ipv6** *ipv6-address* \| **interface** *interface-type interface-number* } | |

## Configuring Whether First-time Authentication is Supported

When the device connects to the SSH server as an SSH client, you can configure whether the device supports first-time authentication.

- With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client will use the saved server host public key to authenticate the server.
- Without first-time authentication, a client not configured with the server host public key will deny to access the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

### Enable the device to support first-time authentication

Follow these steps to enable the device to support first-time authentication:

| To do... | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the device to support first-time authentication | **ssh client first-time enable** | Optional<br>By default, first-time authentication is supported on a client. |

### Disable first-time authentication

For successful authentication of an SSH client not supporting first-time authentication, the server host public key must be configured on the client and the public key name must be specified.

Follow these steps to disable first-time authentication:

| To do... | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Disable first-time authentication support | **undo ssh client first-time** | Optional<br>By default, first-time authentication is supported on a client. |

| To do... | Use the command… | Remarks |
|---|---|---|
| Configure the server public key | Refer to Configuring a Client Public Key | Required<br>The method of configuring server public key on the client is similar to that of configuring client public key on the server. |
| Specify the host public key name of the server | **ssh client authentication server** *server* **assign publickey** *keyname* | Required |

### Establishing a Connection Between the SSH Client and the Server

Follow these steps to establish the connection between the SSH client and the server:

| To do... | | Use the command… | Remarks |
|---|---|---|---|
| Establish a connection between the SSH client and server, and specify the public key algorithm, preferred encryption algorithms, preferred HMAC algorithms and preferred key exchange algorithm | For an IPv4 server | **ssh2** *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Use either command in user view. |
| | For an IPv4 IPv6 server | **ssh2 ipv6** *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | |

## Displaying and Maintaining SSH

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the source IP address or interface currently set for the SFTP client | **display sftp client source** | Available in any view |
| Display the source IP address or interface currently set for the SSH client | **display ssh client source** | Available in any view |
| Display SSH server status information or session information on an SSH server | **display ssh server** { **status** \| **session** } | Available in any view |
| Display the mappings between SSH servers and their host public keys saved on an SSH client | **display ssh server-info** | Available in any view |
| Display information about a specified or all SSH users on the SSH server | **display ssh user-information** [ *username* ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the public keys of the local key pairs | **display public-key local** { **dsa** \| **rsa** } **public** | Available in any view |
| Display the public keys of the SSH peers | **display public-key peer** [ **brief** \| **name** *publickey-name* ] | Available in any view |

**Note**

For information about the **display public-key local** and **display public-key peer** commands, refer to *Public Key Commands* in the *Security Volume*.

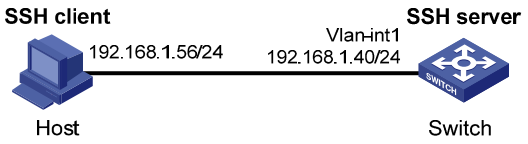
# SSH Server Configuration Examples

## When Switch Acts as Server for Password Authentication

### Network requirements

- As shown in Figure 1-1, a local SSH connection is established between the host (the SSH client) and the switch (the SSH server) for secure data exchange.
- Password authentication is required. The username and password are saved on the switch.

**Figure 1-1** Switch acts as server for password authentication




### Configuration procedure

1) Configure the SSH server

# Generate RSA and DSA key pairs and enable the SSH server.

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# Configure an IP address for VLAN interface 1. This address will serve as the destination of the SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

# Create local user **client001**, and set the user command privilege level to 3

```
[Switch] local-user client001
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh
[Router-luser-client001] authorization-attribute level 3
[Switch-luser-client001] quit
```

# Specify the service type for user **client001** as **Stelnet**, and the authentication mode as password. This step is optional.

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2) Configure the SSH client

---

**Note**

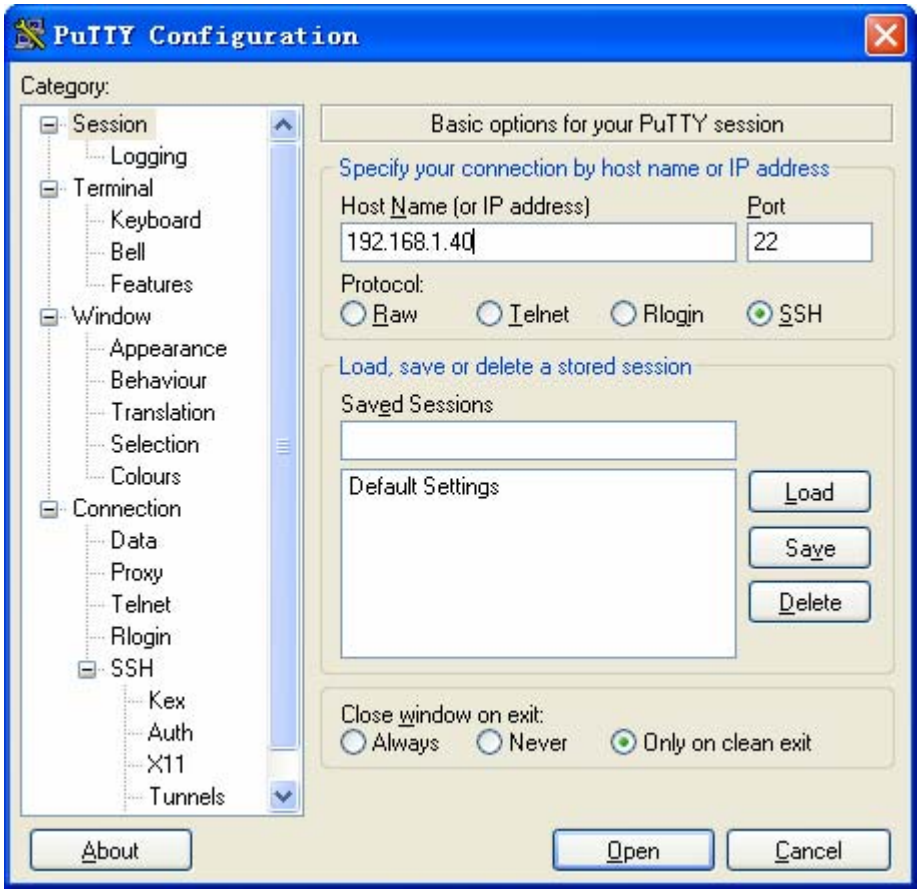
There are many kinds of SSH client software, such as PuTTY, and OpenSSH. The following is an example of configuring SSH client using Putty Version 0.58.

---

# Establish a connection with the SSH server

Launch PuTTY.exe to enter the following interface. In the **Host Name (or IP address)** text box, enter the IP address of the server (192.168.1.40).

**Figure 1-2** SSH client configuration interface



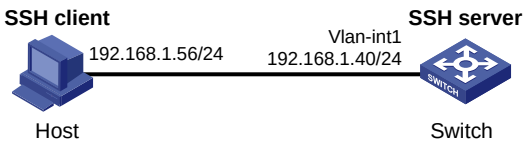

In the window shown in Figure 1-2, click **Open**. If the connection is normal, you will be prompted to enter the username and password. After entering the correct username (**client001**) and password (**aabbcc**), you can enter the configuration interface.

## When Switch Acts as Server for Publickey Authentication

### Network requirements

- As shown in Figure 1-3, a local SSH connection is established between the host (the SSH client) and the switch (the SSH server) for secure data exchange.
- Publickey authentication is used, the algorithm is RSA.

**Figure 1-3** Switch acts as server for publickey authentication




### Configuration procedure

1) Configure the SSH server

# Generate RSA and DSA key pairs and enable SSH server.

```
<Switch> system-view
[Switch] public-key local create rsa
```

```
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# Configure an IP address for VLAN interface 1. This address will serve as the destination of the SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
```

# Set the user command privilege level to 3.

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```

---

**Note**

Before performing the following tasks, you must use the client software to generate an RSA key pair on the client, save the public key in a file named **key.pub**, and then upload the file to the SSH server through FTP or TFTP. For details, refer to Configure the SSH client below.

---

# Import the client's public key from file **key.pub** and name it **Switch001**.

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

# Specify the authentication type for user **client002** as publickey, and assign the public key **Switch001** to the user.

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey Switch001
```

2) Configure the SSH client

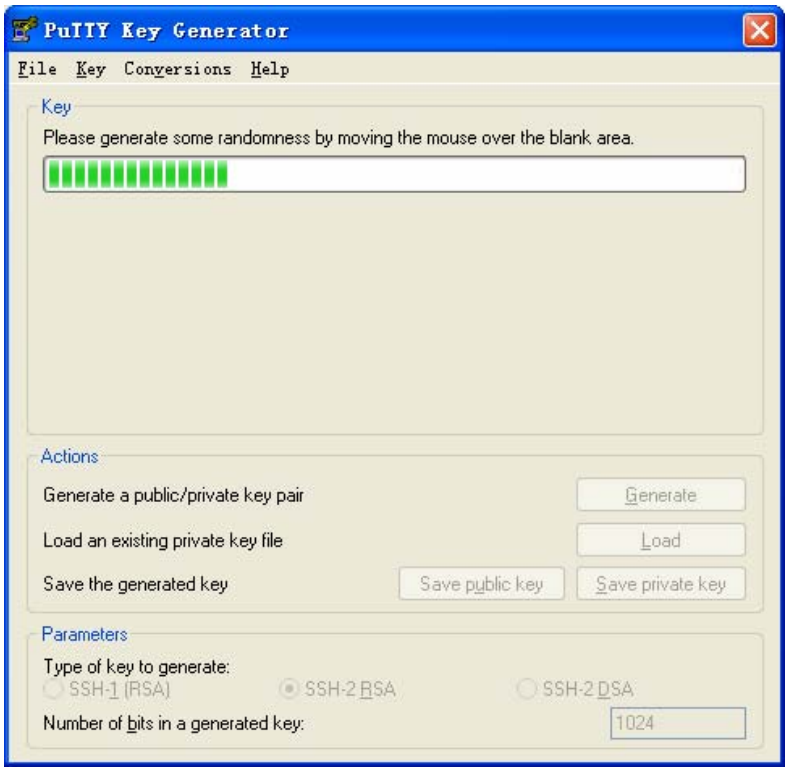
# Generate an RSA key pair.

Run PuTTYGen.exe, select **SSH-2 RSA** and click **Generate**.

**Figure 1-4** Generate a client key pair 1)

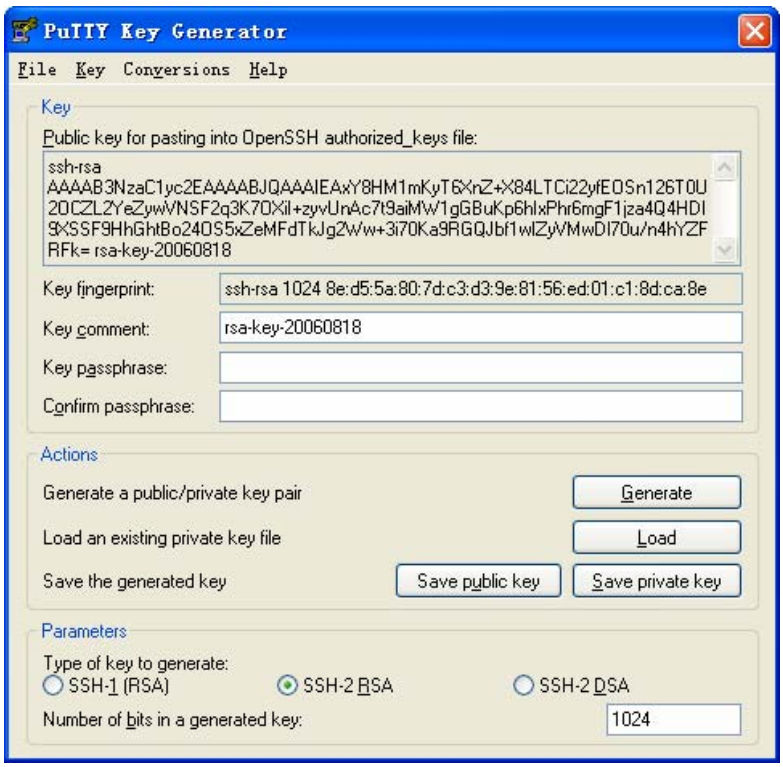

While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in Figure 1-5. Otherwise, the process bar stops moving and the key pair generating process will be stopped.

**Figure 1-5** Generate a client key pair 2)



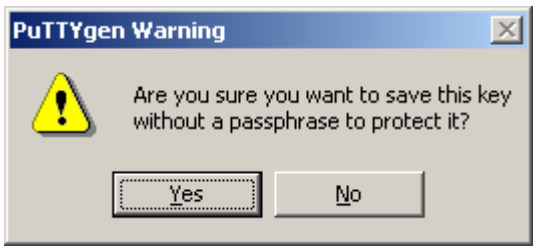

After the key pair is generated, click **Save public key** and specify the file name as **key.pub** to save the public key.

**Figure 1-6** Generate a client key pair 3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the key (**private** in this case).

**Figure 1-7** Generate a client key pair 4)



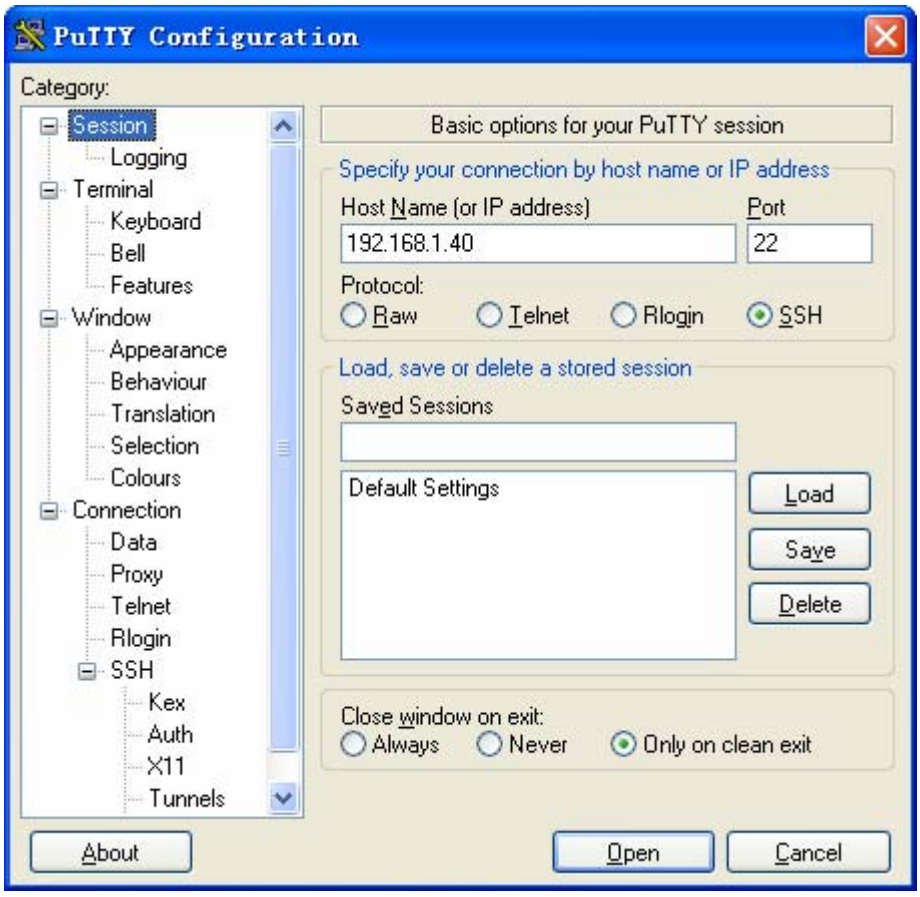

**Note**

After generating a key pair on a client, you need to transmit the saved public key file to the server through FTP or TFTP and have the configuration on the server done before continuing configuration of the client.

# Specify the private key file and establish a connection with the SSH server

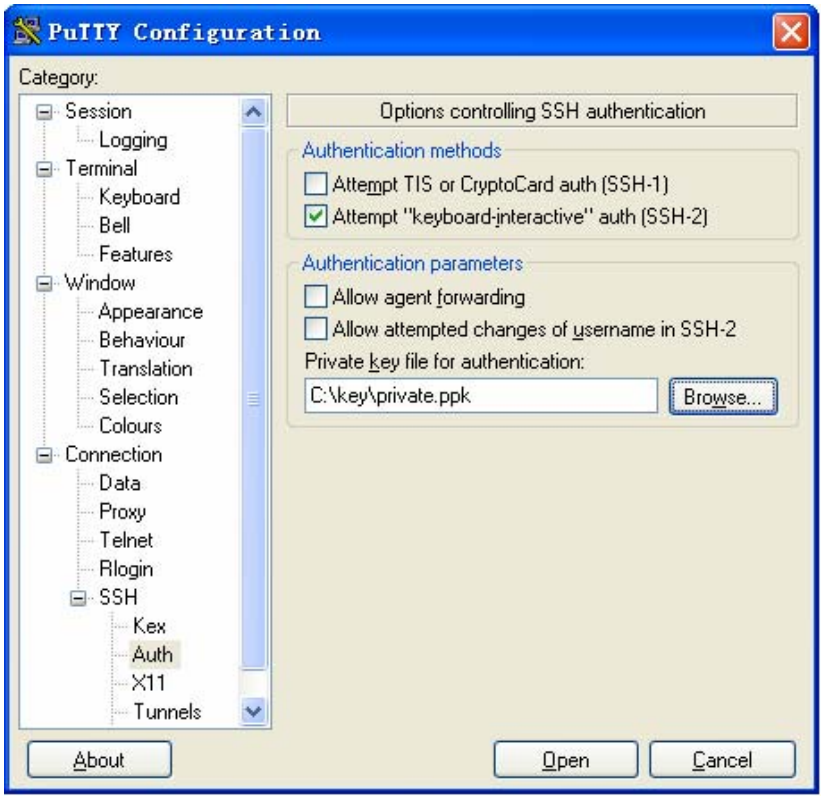
Launch PuTTY.exe to enter the following interface. In the **Host Name (or IP address)** text box, enter the IP address of the server (192.168.1.40).

**Figure 1-8** SSH client configuration interface 1)



Select **Connection/SSH/Auth** from the navigation tree. The following window appears. Click **Browse…** to bring up the file selection window, navigate to the private key file and click **OK**.

**Figure 1-9** SSH client configuration interface 2)




In the window shown in Figure 1-9, click **Open**. If the connection is normal, you will be prompted to enter the username. After entering the correct username (**client002**), you can enter the configuration interface.

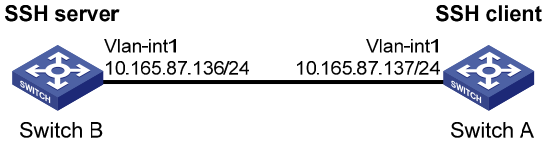
# SSH Client Configuration Examples

## When Switch Acts as Client for Password Authentication

### Network requirements

- As shown in Figure 1-10, Switch A (the SSH client) needs to log into Switch B (the SSH server) through the SSH protocol.
- The username of the SSH client is **client001** and the password is **aabbcc**. Password authentication is required.

**Figure 1-10** Switch acts as client for password authentication




### Configuration procedure

1) Configure the SSH server

# Create RSA and DSA key pairs and enable the SSH server.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

# Create an IP address for VLAN interface 1, which the SSH client will use as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

# Create local user **client001**.

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh
[SwitchB-luser-client001] authorization-attribute level 3
[SwitchB-luser-client001] quit
```

# Specify the service type for user **client001** as **Stelnet**, and the authentication type as **password**. This step is optional.

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

2) Configure the SSH client

# Configure an IP address for VLAN interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] quit
```

- If the client support first-time authentication, you can directly establish a connection from the client to the server.

# Establish an SSH connection to server 10.165.87.136.

```
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
```

After you enter the correct username, you can log into Switch B successfully.

- If the client does not support first-time authentication, you need to perform the following configurations.

# Disable first-time authentication.

```
[SwitchA] undo ssh client first-time
```

# Configure the host public key of the SSH server. You can get the server host public key by using the **display public-key local dsa public** command on the server.

```
[SwitchA] public-key peer key1
[SwitchA-pkey-public-key] public-key-code begin
[SwitchA-pkey-key-code]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-key-code]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-key-code]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-key-code]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[SwitchA-pkey-key-code]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[SwitchA-pkey-key-code]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-key-code]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-key-code]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[SwitchA-pkey-key-code]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[SwitchA-pkey-key-code]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[SwitchA-pkey-key-code]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[SwitchA-pkey-key-code]485348
[SwitchA-pkey-key-code] public-key-code end
[SwitchA-pkey-public-key] peer-public-key end
```

# Specify the host public key for the SSH server (10.165.87.136) as **key1**.

```
[SwitchA] ssh client authentication server 10.165.87.136 assign publickey key1
[SwitchA] quit
```

# Establish an SSH connection to server 10.165.87.136.

```
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
Enter password:
```

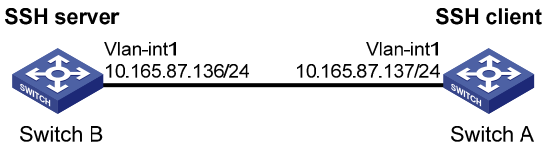
After you enter the correct username and password, you can log into Switch B successfully.

## When Switch Acts as Client for Publickey Authentication

### Network requirements

- As shown in Figure 1-11, Switch A (the SSH client) needs to log into Switch B (the SSH server) through the SSH protocol.
- Publickey authentication is used, and the public key algorithm is DSA.

**Figure 1-11** Switch acts as client for publickey authentication




### Configuration procedure

1) Configure the SSH server

# Generate RSA and DSA key pairs and enable SSH server.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

# Configure an IP address for VLAN interface 1, which the SSH client will use as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

# Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

---

**Note**

Before performing the following tasks, you must use the client software to generate an RSA key pair on the client, save the public key in a file named **key.pub**, and then upload the file to the SSH server through FTP or TFTP. For details, refer to Configure the SSH client below.

---

# Import the peer public key from the file **key.pub**.

```
[SwitchB] public-key peer Switch001 import sshkey key.pub
```

# Specify the authentication type for user **client002** as publickey, and assign the public key **Switch001** to the user.

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey assign publickey Switch001
```

2) Configure the SSH client

# Configure an IP address for Vlan interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

# Generate a DSA key pair.

```
[SwitchA] public-key local create dsa
```

# Export the DSA public key to the file **key.pub**.

```
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```

---

**Note**

After generating a key pair on a client, you need to transmit the saved public key file to the server through FTP or TFTP and have the configuration on the server done before continuing configuration of the client.

---

# Establish an SSH connection to the server (10.165.87.136).

```
<SwitchA> ssh2 10.165.87.136
Username: client002
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

Later, you will find that you have logged into Switch B successfully.

# 2 SFTP Service

When configuring SFTP, go to these sections for information you are interested in:



## SFTP Overview

The secure file transfer protocol (SFTP) is a new feature in SSH2.0.

SFTP uses the SSH connection to provide secure data transfer. The device can serve as the SFTP server, allowing a remote user to log into the SFTP server for secure file management and transfer. The device can also server as an SFTP client, enabling a user to login from the device to a remote device for secure file transfer.

## Configuring an SFTP Server

### Configuration Prerequisites

- You have configured the SSH server. For the detailed configuration procedure, refer to Configuring the Device as an SSH Server.
- You have used the ssh user service-type command to set the service type of SSH users to sftp or all. For configuration procedure, refer to Configuring an SSH User.

### Enabling the SFTP Server

This configuration task is to enable the SFTP service so that a client can log into the SFTP server through SFTP.

Follow these steps to enable the SFTP server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the SFTP server | **sftp server enable** | Required<br>Disabled by default |

**Note**

When the device functions as the SFTP server, only one client can access the SFTP server at a time. If the SFTP client uses WinSCP, a file on the server cannot be modified directly; it can only be downloaded to a local place, modified, and then uploaded to the server.

### Configuring the SFTP Connection Idle Timeout Period

Once the idle period of an SFTP connection exceeds the specified threshold, the system automatically tears the connection down, so that a user cannot occupy a connection for nothing.

Follow these steps to configure the SFTP connection idle timeout period:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the SFTP connection idle timeout period | **sftp server idle-timeout** *time-out-value* | Optional<br>10 minutes by default |

## Configuring an SFTP Client

### Specifying a Source IP Address or Interface for the SFTP Client

You can configure a client to use only a specified source IP address or interface to access the SFTP server, thus enhancing the service manageability.

Follow these steps to specify a source IP address or interface for the SFTP client:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Specify a source IP address or interface for the SFTP client | Specify a source IPv4 address or interface for the SFTP client | **sftp client source** { **ip** *ip-address* \| **interface** *interface-type interface-number* } | Required<br>Use either command.<br>By default, an SFTP client uses the interface address specified by the route of the device to access the SFTP server. |
| | Specify a source IPv6 address or interface for the SFTP client | **sftp client ipv6 source** { **ipv6** *ipv6-address* \| **interface** *interface-type interface-number* } | |

### Establishing a Connection to the SFTP Server

This configuration task is to enable the SFTP client to establish a connection with the remote SFTP server and enter SFTP client view.

Follow these steps to enable the SFTP client:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Establish a connection to the remote SFTP server and enter SFTP client view | Establish a connection to the remote IPv4 SFTP server and enter SFTP client view | **sftp** *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Use either command in user view. |
| | Establish a connection to the remote IPv6 SFTP server and enter SFTP client view | **sftp ipv6** *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | |

## Working with the SFTP Directories

SFTP directory operations include:

- Changing or displaying the current working directory
- Displaying files under a specified directory or the directory information
- Changing the name of a specified directory on the server
- Creating or deleting a directory

Follow these steps to work with the SFTP directories:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter SFTP client view | **sftp** [ **ipv6** ] *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Execute the command in user view. |
| Change the working directory of the remote SFTP server | **cd** [ *remote-path* ] | Optional |
| Return to the upper-level directory | **cdup** | Optional |
| Display the current working directory of the remote SFTP server | **pwd** | Optional |
| Display files under a specified directory | **dir** [ **-a** \| **-l** ] [ *remote-path* ] | Optional<br>The **dir** command functions as the **ls** command. |
| | **ls** [ **-a** \| **-l** ] [ *remote-path* ] | |
| Change the name of a specified directory on the SFTP server | **rename** *oldname newname* | Optional |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a new directory on the remote SFTP server | **mkdir** *remote-path* | Optional |
| Delete a directory from the SFTP server | **rmdir** *remote-path*&<1-10> | Optional |

## Working with SFTP Files

SFTP file operations include:

- Changing the name of a file
- Downloading a file
- Uploading a file
- Displaying a list of the files
- Deleting a file

Follow these steps to work with SFTP files:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter SFTP client view | **sftp** [ **ipv6** ] *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Execute the command in user view. |
| Change the name of a specified file or directory on the SFTP server | **rename** *old-name new-name* | Optional |
| Download a file from the remote server and save it locally | **get** *remote-file* [ *local-file* ] | Optional |
| Upload a local file to the remote SFTP server | **put** *local-file* [ *remote-file* ] | Optional |
| Display the files under a specified directory | **dir** [ **-a** \| **-l** ] [ *remote-path* ] | Optional<br>The **dir** command functions as the **ls** command. |
| | **ls** [ **-a** \| **-l** ] [ *remote-path* ] | |
| Delete a file from the SFTP server | **delete** *remote-file*&<1-10> | Optional<br>The **delete** command functions as the **remove** command. |
| | **remove** *remote-file*&<1-10> | |

## Displaying Help Information

This configuration task is to display a list of all commands or the help information of an SFTP client command, such as the command format and parameters.

Follow these steps to display a list of all commands or the help information of an SFTP client command:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter SFTP client view | **sftp** [ **ipv6** ] *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Execute the command in user view. |
| Display a list of all commands or the help information of an SFTP client command | **help** [ **all** \| *command-name* ] | Required |

### Terminating the Connection to the Remote SFTP Server

Follow these steps to terminate the connection to the remote SFTP server:

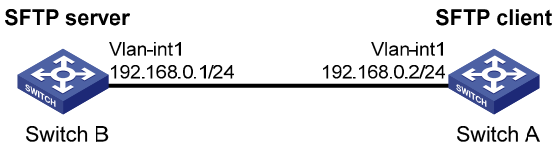
| To do… | Use the command… | Remarks |
|---|---|---|
| Enter SFTP client view | **sftp** [ **ipv6** ] *server* [ *port-number* ] [ **identity-key** { **dsa** \| **rsa** } \| **prefer-ctos-cipher** { **aes128** \| **des** } \| **prefer-ctos-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } \| **prefer-kex** { **dh-group-exchange** \| **dh-group1** \| **dh-group14** } \| **prefer-stoc-cipher** { **aes128** \| **des** } \| **prefer-stoc-hmac** { **md5** \| **md5-96** \| **sha1** \| **sha1-96** } ] * | Required<br>Execute the command in user view. |
| Terminate the connection to the remote SFTP server and return to user view | **bye** | Required.<br>Use any of the commands.<br>These three commands function in the same way. |
| | **exit** | |
| | **quit** | |

## SFTP Client Configuration Example

### Network requirements

As shown in Figure 2-1, an SSH connection is established between Switch A and Switch B. Switch A, an SFTP client, logs in to Switch B for file management and file transfer. An SSH user uses publickey authentication with the public key algorithm being RSA.

**Figure 2-1** Network diagram for SFTP client configuration




### Configuration procedure

1) Configure the SFTP server (Switch B)

# Generate RSA and DSA key pairs and enable the SSH server.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

# Enable the SFTP server.

```
[SwitchB] sftp server enable
```

# Configure an IP address for VLAN interface 1, which the SSH client uses as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode on the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

# Set the protocol that a remote user uses to log in as **SSH**.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

---

 **Note**

Before performing the following tasks, you must generate use the client software to generate RSA key pairs on the client, save the host public key in a file named **pubkey**, and then upload the file to the SSH server through FTP or TFTP. For details, refer to Configure the SFTP client (Switch A) below.

---

# Import the peer public key from the file **pubkey**.

```
[SwitchB] public-key peer Switch001 import sshkey pubkey
```

# For user **client001**, set the service type as SFTP, authentication type as publickey, public key as **Switch001**, and working folder as **flash:/**

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign publickey Switch001 work-directory flash:/
```

2) Configure the SFTP client (Switch A)

# Configure an IP address for VLAN interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

# Generate RSA key pairs.

```
[SwitchA] public-key local create rsa
```

# Export the host public key to file **pubkey**.

```
[SwitchA] public-key local export rsa ssh2 pubkey
```

```
[SwitchA] quit
```

**Note**

After generating key pairs on a client, you need to transmit the saved public key file to the server through FTP or TFTP and have the configuration on the server done before continuing configuration of the client.

# Establish a connection to the remote SFTP server and enter SFTP client view.

```
<SwitchA> sftp 192.168.0.1 identity-key rsa
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n

sftp-client>
```

# Display files under the current directory of the server, delete the file named **z**, and check if the file has been deleted successfully.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp-client> delete z
The following File will be deleted:
/z
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

# Add a directory named **new1** and check if it has been created successfully.

```
sftp-client> mkdir new1
New directory created
```

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

# Rename directory **new1** to **new2** and check if the directory has been renamed successfully.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

# Download the file **pubkey2** from the server and change the name to **public**.

```
sftp-client> get pubkey2 public
Remote  file:/pubkey2 --->  Local file: public
Downloading file successfully ended
```

# Upload the local file **pu** to the server, save it as **puk**, and check if the file has been uploaded successfully.

```
sftp-client> put pu puk
Local file:pu --->  Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp-client>
```

# Terminate the connection to the remote SFTP server.

```
sftp-client> quit
Bye
<SwitchA>
```

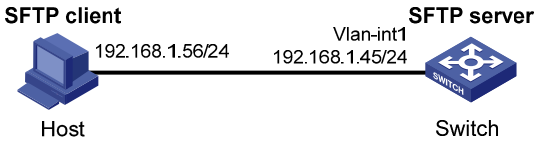
# SFTP Server Configuration Example

## Network requirements

As shown in Figure 2-2, an SSH connection is established between the host and the switch. The host, an SFTP client, logs into the switch for file management and file transfer. An SSH user uses password

authentication with the username being **client002** and the password being **aabbcc**. The username and password are saved on the switch.

**Figure 2-2** Network diagram for SFTP server configuration




## Configuration procedure

1) Configure the SFTP server

# Generate RSA and DSA key pairs and enable the SSH server.

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# Enable the SFTP server.

```
[Switch] sftp server enable
```

# Configure an IP address for VLAN-interface 1, which the client will use as the destination for SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode of the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

# Configure a local user named **client002** with the password being **aabbcc** and the service type being SSH.

```
[Switch] local-user client002
[Switch-luser-client002] password simple aabbcc
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] quit
```

# Configure the user authentication type as password and service type as SFTP.

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

2) Configure the SFTP client

**Note**

- There are many kinds of SSH client software. The following takes the PSFTP of Putty Version 0.58 as an example.
- The PSFTP supports only password authentication.

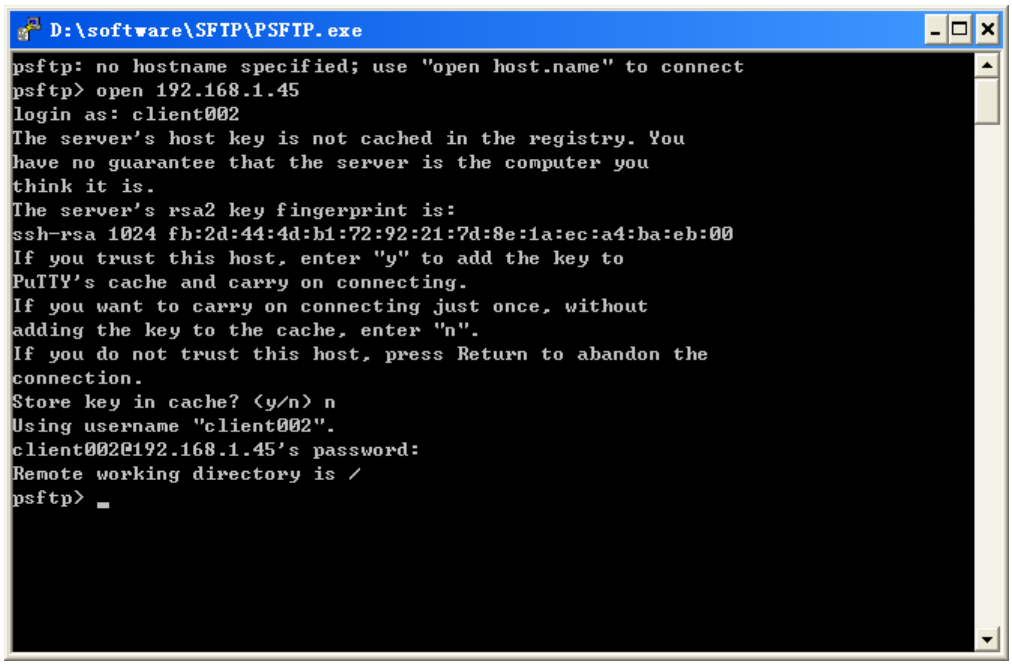
# Establish a connection with the remote SFTP server.

Run the psftp.exe to launch the client interface as shown in Figure 2-3, and enter the following command:

```
open 192.168.1.45
```

Enter username **client002** and password **aabbcc** as prompted to log into the SFTP server.

**Figure 2-3** SFTP client interface



# Table of Contents

# 1 PKI Configuration

When configuring PKI, go to these sections for information you are interested in:



## Introduction to PKI

This section covers these topics:



### PKI Overview

The Public Key Infrastructure (PKI) is a general security infrastructure for providing information security through public key technologies.

PKI, also called asymmetric key infrastructure, uses a key pair to encrypt and decrypt the data. The key pair consists of a private key and a public key. The private key must be kept secret while the public key needs to be distributed. Data encrypted by one of the two keys can only be decrypted by the other.

A key problem of PKI is how to manage the public keys. Currently, PKI employs the digital certificate mechanism to solve this problem. The digital certificate mechanism binds public keys to their owners, helping distribute public keys in large networks securely.

With digital certificates, the PKI system provides network communication and e-commerce with security services such as user authentication, data non-repudiation, data confidentiality, and data integrity.

### PKI Terms

#### Digital certificate

A digital certificate is a file signed by a certificate authority (CA) for an entity. It includes mainly the identity information of the entity, the public key of the entity, the name and signature of the CA, and the validity period of the certificate, where the signature of the CA ensures the validity and authority of the certificate. A digital certificate must comply with the international standard of ITU-T X.509. Currently, the most common standard is X.509 v3.

This manual involves two types of certificates: local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity, while a CA certificate is the certificate of a CA. If multiple CAs are trusted by different users in a PKI system, the CAs will form a CA tree with the root CA at the top

level. The root CA has a CA certificate signed by itself while each lower level CA has a CA certificate signed by the CA at the next higher level.

### CRL

An existing certificate may need to be revoked when, for example, the user name changes, the private key leaks, or the user stops the business. Revoking a certificate is to remove the binding of the public key with the user identity information. In PKI, the revocation is made through certificate revocation lists (CRLs). Whenever a certificate is revoked, the CA publishes one or more CRLs to show all certificates that have been revoked. The CRLs contain the serial numbers of all revoked certificates and provide an effective way for checking the validity of certificates.

A CA may publish multiple CRLs when the number of revoked certificates is so large that publishing them in a single CRL may degrade network performance, and it uses CRL distribution points to indicate the URLs of these CRLs.

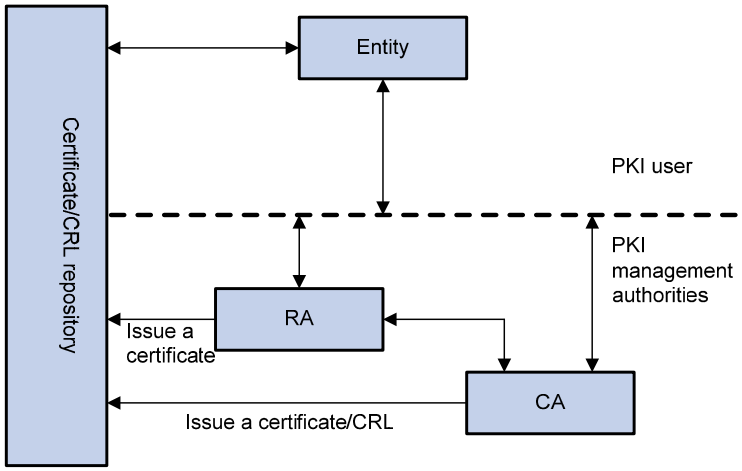
### CA policy

A CA policy is a set of criteria that a CA follows in processing certificate requests, issuing and revoking certificates, and publishing CRLs. Usually, a CA advertises its policy in the form of certification practice statement (CPS). A CA policy can be acquired through out-of-band means such as phone, disk, and e-mail. As different CAs may use different methods to check the binding of a public key with an entity, make sure that you understand the CA policy before selecting a trusted CA for certificate request.

## Architecture of PKI

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository, as shown in Figure 1-1.

**Figure 1-1** PKI architecture




### Entity

An entity is an end user of PKI products or services, such as a person, an organization, a device like a router or a switch, or a process running on a computer.

### CA

A CA is a trusted authority responsible for issuing and managing digital certificates. A CA issues certificates, specifies the validity periods of certificates, and revokes certificates as needed by publishing CRLs.

### RA

A registration authority (RA) is an extended part of a CA or an independent authority. An RA can implement functions including identity authentication, CRL management, key pair generation and key pair backup. The PKI standard recommends that an independent RA be used for registration management to achieve higher security of application systems.

### PKI repository

A PKI repository can be a Lightweight Directory Access Protocol (LDAP) server or a common database. It stores and manages information like certificate requests, certificates, keys, CRLs and logs while providing a simple query function.

LDAP is a protocol for accessing and managing PKI information. An LDAP server stores user information and digital certificates from the RA server and provides directory navigation service. From an LDAP server, an entity can retrieve local and CA certificates of its own as well as certificates of other entities.

## Applications of PKI

The PKI technology can satisfy the security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

### VPN

A virtual private network (VPN) is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for instance, IPSec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.

### Secure E-mail

E-mails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure E-mail protocol that is currently developing rapidly is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

### Web security

For Web security, two peers can establish a Secure Sockets Layer (SSL) connection first for transparent and secure communications at the application layer. With PKI, SSL enables encrypted communications between a browser and a server. Both the communication parties can verify the identity of each other through digital certificates.

## Operation of PKI

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificates. Here is how it works:

1) An entity submits a certificate request to the RA.

2) The RA reviews the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.
3) The CA verifies the digital signature, approves the application, and issues a certificate.
4) The RA receives the certificate from the CA, sends it to the LDAP server to provide directory navigation service, and notifies the entity that the certificate is successfully issued.
5) The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.
6) The entity makes a request to the CA when it needs to revoke its certificate, while the CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

## PKI Configuration Task List

Complete the following tasks to configure PKI:

| Task | | Remarks |
|---|---|---|
| Configuring an Entity DN | | Required |
| Configuring a PKI Domain | | Required |
| Submitting a PKI Certificate Request | Submitting a Certificate Request in Auto Mode | Required<br>Use either approach |
| | Submitting a Certificate Request in Manual Mode | |
| Retrieving a Certificate Manually | | Optional |
| Configuring PKI Certificate | | Optional |
| Destroying a Local RSA Key Pair | | Optional |
| Deleting a Certificate | | Optional |
| Configuring an Access Control Policy | | Optional |

## Configuring an Entity DN

A certificate is the binding of a public key and the identity information of an entity, where the identity information is identified by an entity distinguished name (DN). A CA identifies a certificate applicant uniquely by entity DN.

An entity DN is defined by these parameters:

- Common name of the entity.
- Country code of the entity, a standard 2-character code. For example, CN represents China and US represents the United States of America.
- Fully qualified domain name (FQDN) of the entity, a unique identifier of an entity on the network. It consists of a host name and a domain name and can be resolved to an IP address. For example, www.whatever.com is an FQDN, where www is a host name and whatever.com a domain name.
- IP address of the entity.
- Locality where the entity resides.
- Organization to which the entity belongs.
- Unit of the entity in the organization.
- State where the entity resides.

**Note**

The configuration of an entity DN must comply with the CA certificate issue policy. You need to determine, for example, which entity DN parameters are mandatory and which are optional. Otherwise, certificate request may be rejected.

Follow these steps to configure an entity DN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an entity and enter its view | **pki entity** *entity-name* | Required<br>No entity exists by default. |
| Configure the common name for the entity | **common-name** *name* | Optional<br>No common name is specified by default. |
| Configure the country code for the entity | **country** *country-code-str* | Optional<br>No country code is specified by default. |
| Configure the FQDN for the entity | **fqdn** *name-str* | Optional<br>No FQDN is specified by default. |
| Configure the IP address for the entity | **ip** *ip-address* | Optional<br>No IP address is specified by default. |
| Configure the locality of the entity | **locality** *locality-name* | Optional<br>No locality is specified by default. |
| Configure the organization name for the entity | **organization** *org-name* | Optional<br>No organization is specified by default. |
| Configure the unit name for the entity | **organization-unit** *org-unit-name* | Optional<br>No unit is specified by default. |
| Configure the state or province for the entity | **state** *state-name* | Optional<br>No state or province is specified by default. |

**Note**

- Currently, up to two entities can be created on a device.
- The Windows 2000 CA server has some restrictions on the data length of a certificate request. If the entity DN in a certificate request goes beyond a certain limit, the server will not respond to the certificate request.

# Configuring a PKI Domain

Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain. A PKI domain is intended only for convenience of reference by other applications like IKE and SSL, and has only local significance.

A PKI domain is defined by these parameters:

- Trusted CA

An entity requests a certificate from a trusted CA.

- Entity

A certificate applicant uses an entity to provide its identity information to a CA.

- RA

Generally, an independent RA is in charge of certificate request management. It receives the registration request from an entity, checks its qualification, and determines whether to ask the CA to sign a digital certificate. The RA only checks the application qualification of an entity; it does not issue any certificate. Sometimes, the registration management function is provided by the CA, in which case no independent RA is required. You are recommended to deploy an independent RA.

- URL of the registration server

An entity sends a certificate request to the registration server through Simple Certification Enrollment Protocol (SCEP), a dedicated protocol for an entity to communicate with a CA.

- Polling interval and count

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed. You can configure the polling interval and count to query the request status.

- IP address of the LDAP server

An LDAP server is usually deployed to store certificates and CRLs. If this is the case, you need to configure the IP address of the LDAP server.

- Fingerprint for root certificate verification

Upon receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate, namely, the hash value of the root certificate content. This hash value is unique to every certificate. If the fingerprint of the root certificate does not match the one configured for the PKI domain, the entity will reject the root certificate.

Follow these steps to configure a PKI domain:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a PKI domain and enter its view | **pki domain** *domain-name* | Required<br>No PKI domain exists by default. |
| Specify the trusted CA | **ca identifier** *name* | Required<br>No trusted CA is specified by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify the entity for certificate request | **certificate request entity** *entity-name* | Required<br>No entity is specified by default.<br>The specified entity must exist. |
| Specify the authority for certificate request | **certificate request from** { **ca** \| **ra** } | Required<br>No authority is specified by default. |
| Configure the URL of the server for certificate request | **certificate request url** *url-string* | Required<br>No URL is configured by default. |
| Configure the polling interval and attempt limit for querying the certificate request status | **certificate request polling** { **count** *count* \| **interval** *minutes* } | Optional<br>The polling is executed for up to 50 times at the interval of 20 minutes by default. |
| Specify the LDAP server | **ldap-server ip** *ip-address* [ **port** *port-number* ] [ **version** *version-number* ] | Optional<br>No LDP server is specified by default. |
| Configure the fingerprint for root certificate verification | **root-certificate fingerprint** { **md5** \| **sha1** } *string* | Required when the certificate request mode is auto and optional when the certificate request mode is manual. In the latter case, if you do not configure this command, the fingerprint of the root certificate must be verified manually.<br>No fingerprint is configured by default. |

**Note**

- Currently, up to two PKI domains can be created on a device.
- The CA name is required only when you retrieve a CA certificate. It is not used when in local certificate request.
- Currently, the URL of the server for certificate request does not support domain name resolving.

# Submitting a PKI Certificate Request

When requesting a certificate, an entity introduces itself to the CA by providing its identity information and public key, which will be the major components of the certificate. A certificate request can be submitted to a CA in two ways: online and offline. In offline mode, a certificate request is submitted to a CA by an “out-of-band” means such as phone, disk, or e-mail.

Online certificate request falls into two categories: manual mode and auto mode.

## Submitting a Certificate Request in Auto Mode

In auto mode, an entity automatically requests a certificate through the SCEP protocol when it has no local certificate or the present certificate is about to expire.

Follow these steps to configure an entity to submit a certificate request in auto mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter PKI domain view | **pki domain** *domain-name* | — |
| Set the certificate request mode to auto | **certificate request mode auto** [ **key-length** *key-length* \| **password** { **cipher** \| **simple** } *password* ] * | Required<br>Manual by default |

## Submitting a Certificate Request in Manual Mode

In manual mode, you need to retrieve a CA certificate, generate a local RSA key pair, and submit a local certificate request for an entity.

The goal of retrieving a CA certificate is to verify the authenticity and validity of a local certificate.

Generating an RSA key pair is an important step in certificate request. The key pair includes a public key and a private key. The private key is kept by the user, while the public key is transferred to the CA along with some other information. For detailed information about RSA key pair configuration, refer to *Public Key Configuration* in the *Security Volume*.

Follow these steps to submit a certificate request in manual mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter PKI domain view | **pki domain** *domain-name* | — |
| Set the certificate request mode to manual | **certificate request mode manual** | Optional<br>Manual by default |
| Return to system view | **quit** | — |
| Retrieve a CA certificate manually | Refer to Retrieving a Certificate Manually | Required |
| Generate a local RSA key pair | **public-key local create rsa** | Required<br>No local RSA key pair exists by default. |
| Submit a local certificate request manually | **pki request-certificate domain** *domain-name* [ *password* ] [ **pkcs10** [ **filename** *filename* ] ] | Required |

**Note**

- If a PKI domain already has a local certificate, creating an RSA key pair will result in inconsistency between the key pair and the certificate. To generate a new RSA key pair, delete the local certificate and then issue the **public-key local create** command. For information about the **public-key local create** command, refer to *Public Key Commands* in the *Security Volume*.
- A newly created key pair will overwrite the existing one. If you perform the **public-key local create** command in the presence of a local RSA key pair, the system will ask you whether you want to overwrite the existing one.
- If a PKI domain has already a local certificate, you cannot request another certificate for it. This is to avoid inconsistency between the certificate and the registration information resulting from configuration changes. To request a new certificate, use the **pki delete-certificate** command to delete the existing local certificate and the CA certificate stored locally.
- When it is impossible to request a certificate from the CA through SCEP, you can save the request information by using the **pki request-certificate domain** command with the **pkcs10** and **filename** keywords, and then send the file to the CA by an out-of-band means.
- Make sure the clocks of the entity and the CA are synchronous. Otherwise, the validity period of the certificate will be abnormal.
- The **pki request-certificate domain** configuration will not be saved in the configuration file.

## Retrieving a Certificate Manually

You can download an existing CA certificate, local certificate, or peer entity certificate from the CA server and save it locally. To do so, you can use two ways: online and offline. In offline mode, you need to retrieve a certificate by an out-of-band means like FTP, disk, e-mail and then import it into the local PKI system.

Certificate retrieval serves two purposes:

- Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count,
- Prepare for certificate verification.

Before retrieving a local certificate in online mode, be sure to complete LDAP server configuration.

Follow these steps to retrieve a certificate manually:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Retrieve a certificate manually | Online | **pki retrieval-certificate** { **ca** \| **local** } **domain** *domain-name* | Required<br>Use either command. |
| | Offline | **pki import-certificate** { **ca** \| **local** } **domain** *domain-name* { **der** \| **p12** \| **pem** } [ **filename** *filename* ] | |

**Caution**

- If a PKI domain already has a CA certificate, you cannot retrieve another CA certificate for it. This is in order to avoid inconsistency between the certificate and registration information due to related configuration changes. To retrieve a new CA certificate, use the **pki delete-certificate** command to delete the existing CA certificate and local certificate first.
- The **pki retrieval-certificate** configuration will not be saved in the configuration file.

# Configuring PKI Certificate Verification

A certificate needs to be verified before being used. Verifying a certificate is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Before verifying a certificate, you need to retrieve the CA certificate.

You can specify whether CRL checking is required in certificate verification. If you enable CRL checking, CRLs will be used in verification of a certificate.

## Configuring CRL-checking-enabled PKI certificate verification

Follow these steps to configure CRL-checking-enabled PKI certificate verification:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter PKI domain view | **pki domain** *domain-name* | — |
| Specify the URL of the CRL distribution point | **crl url** *url-string* | Optional<br>No CRL distribution point URL is specified by default. |
| Set the CRL update period | **crl update-period** *hours* | Optional<br>By default, the CRL update period depends on the next update field in the CRL file. |
| Enable CRL checking | **crl check enable** | Optional<br>Enabled by default |
| Return to system view | **quit** | — |
| Retrieve the CA certificate | Refer to Retrieving a Certificate Manually | Required |
| Retrieve CRLs | **pki retrieval-crl domain** *domain-name* | Required |
| Verify the validity of a certificate | **pki validate-certificate** { **ca** \| **local** } **domain** *domain-name* | Required |

## Configuring CRL-checking-disabled PKI certificate verification

Follow these steps to configure CRL-checking-disabled PKI certificate verification:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter PKI domain view | **pki domain** *domain-name* | — |
| Disable CRL checking | **crl check disable** | Required<br>Enabled by default |
| Return to system view | **quit** | — |
| Retrieve the CA certificate | Refer to Retrieving a Certificate Manually | Required |
| Verify the validity of the certificate | **pki validate-certificate** { **ca** \| **local** } **domain** *domain-name* | Required |

**Note**

- The CRL update period refers to the interval at which the entity downloads CRLs from the CRL server. The CRL update period configured manually is prior to that specified in the CRLs.
- The **pki retrieval-crl domain** configuration will not be saved in the configuration file.
- Currently, the URL of the CRL distribution point does not support domain name resolving.

## Destroying a Local RSA Key Pair

A certificate has a lifetime, which is determined by the CA. When the private key leaks or the certificate is about to expire, you can destroy the old RSA key pair and then create a pair to request a new certificate.

Follow these steps to destroy a local RSA key pair:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Destroy a local RSA key pair | **public-key local destroy rsa** | Required |

**Note**

For details about the **public-key local destroy** command, refer to *Public Key Commands* in the *Security Volume*.

## Deleting a Certificate

When a certificate requested manually is about to expire or you want to request a new certificate, you can delete the current local certificate or CA certificate.

Follow these steps to delete a certificate:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Delete certificates | **pki delete-certificate** { **ca** \| **local** } **domain** *domain-name* | Required |

## Configuring an Access Control Policy

By configuring a certificate attribute-based access control policy, you can further control access to the server, providing additional security for the server.

Follow these steps to configure a certificate attribute-based access control policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a certificate attribute group and enter its view | **pki certificate attribute-group** *group-name* | Required<br>No certificate attribute group exists by default. |
| Configure an attribute rule for the certificate issuer name, certificate subject name, or alternative subject name | **attribute** *id* { **alt-subject-name** { **fqdn** \| **ip** } \| { **issuer-name** \| **subject-name** } { **dn** \| **fqdn** \| **ip** } } { **ctn** \| **equ** \| **nctn** \| **nequ** } *attribute-value* | Optional<br>There is no restriction on the issuer name, certificate subject name and alternative subject name by default. |
| Return to system view | **quit** | — |
| Create a certificate attribute-based access control policy and enter its view | **pki certificate access-control-policy** *policy-name* | Required<br>No access control policy exists by default. |
| Configure a certificate attribute-based access control rule | **rule** [ *id* ] { **deny** \| **permit** } *group-name* | Required<br>No access control rule exists by default. |

**Caution**

A certificate attribute group must exist to be associated with a rule.

## Displaying and Maintaining PKI

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the contents or request status of a certificate | **display pki certificate** { { **ca** \| **local** } **domain** *domain-name* \| **request-status** } | Available in any view |
| Display CRLs | **display pki crl domain** *domain-name* | Available in any view |
| Display information about one or all certificate attribute groups | **display pki certificate attribute-group** { *group-name* \| **all** } | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about one or all certificate attribute-based access control policies | **display pki certificate access-control-policy** { *policy-name* \| **all** } | Available in any view |

# PKI Configuration Examples

**Caution**

- The SCEP plug-in is required when you use the Windows Server as the CA. In this case, when configuring the PKI domain, you need to use the **certificate request from ra** command to specify that the entity requests a certificate from an RA.
- The SCEP plug-in is not required when RSA Keon is used. In this case, when configuring a PKI domain, you need to use the **certificate request from ca** command to specify that the entity requests a certificate from a CA.

## Requesting a Certificate from a CA Running RSA Keon

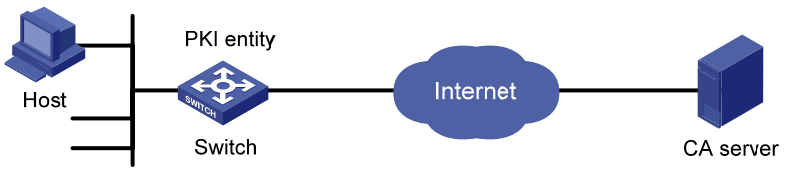
**Note**

The CA server runs RSA Keon in this configuration example.

### Network requirements

- The device submits a local certificate request to the CA server.
- The device acquires the CRLs for certificate verification.

**Figure 1-2** Request a certificate from a CA running RSA Keon




### Configuration procedure

1) Configure the CA server

# Create a CA server named **myca**.

In this example, you need to configure these basic attributes on the CA server at first:

- Nickname: Name of the trusted CA.

- Subject DN: DN information of the CA, including the Common Name (CN), Organization Unit (OU), Organization (O), and Country (C).

The other attributes may be left using the default values.

# Configure extended attributes.

After configuring the basic attributes, you need to perform configuration on the jurisdiction configuration page of the CA server. This includes selecting the proper extension profiles, enabling the SCEP autovetting function, and adding the IP address list for SCEP autovetting.

# Configure the CRL distribution behavior.

After completing the above configuration, you need to perform CRL related configurations. In this example, select the local CRL distribution mode of HTTP and set the HTTP URL to http://4.4.4.133:447/myca.crl.

After the above configuration, make sure that the system clock of the device is synchronous to that of the CA, so that the device can request certificates and retrieve CRLs properly.

2) Configure the switch

- Configure the entity DN

# Configure the entity name as **aaa** and the common name as **switch**.

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

# Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

# Configure the name of the trusted CA as **myca**.

```
[Switch-pki-domain-torsa] ca identifier myca
```

# Configure the URL of the registration server in the format of http://host:port/Issuing Jurisdiction ID, where Issuing Jurisdiction ID is a hexadecimal string generated on the CA server.

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

# Set the registration authority to **CA**.

```
[Switch-pki-domain-torsa] certificate request from ca
```

# Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

# Configure the URL for the CRL distribution point.

```
[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Switch-pki-domain-torsa] quit
```

- Generate a local key pair using RSA

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
```

```
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
```

- Apply for certificates

# Retrieve the CA certificate and save it locally.

```
[Switch] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

# Retrieve CRLs and save them locally.

```
[Switch] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!
```

# Request a local certificate manually.

```
[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Switch]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

3) Verify your configuration

# Use the following command to view information about the local certificate acquired.

```
<Switch> display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9A96A48F 9A509FD7 05FFF4DF 104AD094
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=cn
            O=org
            OU=test
            CN=myca
        Validity
            Not Before: Jan  8 09:26:53 2007 GMT
```

```
            Not After : Jan  8 09:26:53 2008 GMT
        Subject:
            CN=switch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00D67D50 41046F6A 43610335 CA6C4B11
                    F8F89138 E4E905BD 43953BA2 623A54C0
                    EA3CB6E0 B04649CE C9CDDD38 34015970
                    981E96D9 FF4F7B73 A5155649 E583AC61
                    D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
                    D1D8B08A DBF16205 7C2A4011 05F11094
                    73EB0549 A65D9E74 0F2953F2 D4F0042F
                    19103439 3D4F9359 88FB59F3 8D4B2F6C
                    2B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:
            URI:http://4.4.4.133:447/myca.crl

    Signature Algorithm: sha1WithRSAEncryption
        836213A4 F2F74C1A 50F4100D B764D6CE
        B30C0133 C4363F2F 73454D51 E9F95962
        EDE9E590 E7458FA6 765A0D3F C4047BC2
        9C391FF0 7383C4DF 9A0CCFA9 231428AF
        987B029C C857AD96 E4C92441 9382E798
        8FCC1E4A 3E598D81 96476875 E2F86C33
        75B51661 B6556C5E 8F546E97 5197734B
        C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C
```

You can also use some other **display** commands to view detailed information about the CA certificate and CRLs. Refer to the parts related to **display pki certificate ca domain** and **display pki crl domain** commands in *PKI Commands* of the *Security Volume*.

## Requesting a Certificate from a CA Running Windows 2003 Server

---

 **Note**

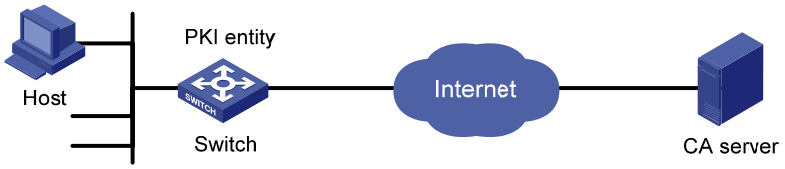
The CA server runs the Windows 2003 server in this configuration example.

---

### Network requirements

Configure PKI entity Switch to request a local certificate from the CA server.

**Figure 1-3** Request a certificate from a CA running Windows 2003 server




## Configuration procedure

1) Configure the CA server

- Install the certificate server suites

From the start menu, select **Control Panel** > **Add or Remove Programs**, and then select **Add/Remove Windows Components** > **Certificate Services** and click **Next** to begin the installation.

- Install the SCEP plug-in

As a CA server running the Windows 2003 server does not support SCEP by default, you need to install the SCEP plug-in so that the switch can register and obtain its certificate automatically. After the SCEP plug-in installation completes, a URL is displayed, which you need to configure on the switch as the URL of the server for certificate registration.

- Modify the certificate service attributes

From the start menu, select **Control Panel** > **Administrative Tools** > **Certificate Authority**. If the CA server and SCEP plug-in have been installed successfully, there should be two certificates issued by the CA to the RA. Right-click on the CA server in the navigation tree and select **Properties** > **Policy Module**. Click **Properties** and then select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.

- Modify the Internet Information Services (IIS) attributes

From the start menu, select **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager** and then select **Web Sites** from the navigation tree. Right-click on **Default Web Site** and select **Properties** > **Home Directory**. Specify the path for certificate service in the **Local path** text box. In addition, you are recommended to specify an available port number as the TCP port number of the default Web site to avoid conflict with existing services.

After completing the above configuration, check that the system clock of the switch is synchronous to that of the CA server, ensuring that the switch can request a certificate normally.

2) Configure the switch

- Configure the entity DN

# Configure the entity name as **aaa** and the common name as **switch**.

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

# Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

# Configure the name of the trusted CA as **myca**.

```
[Switch-pki-domain-torsa] ca identifier myca
```

# Configure the URL of the registration server in the format of http://host:port/ certsrv/mscep/mscep.dll, where host:port indicates the IP address and port number of the CA server.

```
[Switch-pki-domain-torsa]              certificate              request              url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

# Set the registration authority to **RA**.

```
[Switch-pki-domain-torsa] certificate request from ra
```

# Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

- Generate a local key pair using RSA

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
.
```

- Apply for certificates

# Retrieve the CA certificate and save it locally.

```
[Switch] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
    SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

# Request a local certificate manually.

```
[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Switch]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

3) Verify your configuration

# Use the following command to view information about the local certificate acquired.

```
<Switch> display pki certificate local domain torsa
Certificate:
```

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=CA server
        Validity
            Not Before: Nov 21 12:32:16 2007 GMT
            Not After : Nov 21 12:42:16 2008 GMT
        Subject:
            CN=switch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                    5AEE52AE 14A392E4 E0E5D458 0D341113
                    0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                    10242FDD D3947F5E 2DA70BD9 1FAF07E5
                    1D167CE1 FC20394F 476F5C08 C5067DF9
                    CB4D05E6 55DC11B6 9F4C014D EA600306
                    81D403CF 2D93BC5A 8AF3224D 1125E439
                    78ECEFE1 7FA9AE7B 877B50B8 3280509F
                    6B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
            X509v3 Authority Key Identifier:
            keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

            X509v3 CRL Distribution Points:
            URI:http://l00192b/CertEnroll/CA%20server.crl
            URI:file://\\l00192b\CertEnroll\CA server.crl

            Authority Information Access:
            CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
            CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
        81029589 7BFA1CBD 20023136 B068840B
(Omitted)
```

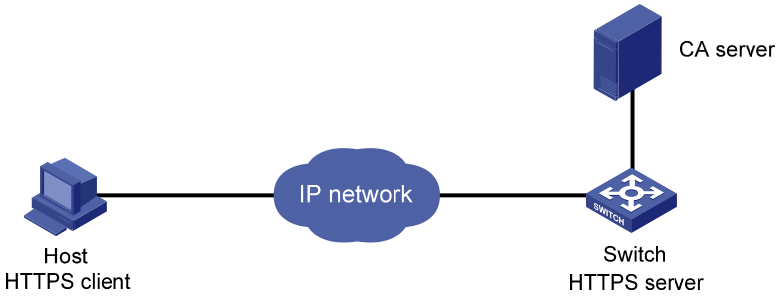
You can also use some other **display** commands to view detailed information about the CA certificate. Refer to the **display pki certificate ca domain** command in *PKI Commands* of the *Security Volume*.

## Configuring a Certificate Attribute-Based Access Control Policy

### Network requirements

- The client accesses the remote HTTP Security (HTTPS) server through the HTTPS protocol.
- SSL is configured to ensure that only legal clients log into the HTTPS server.
- Create a certificate attribute-based access control policy to control access to the HTTPS server.

**Figure 1-4** Configure a certificate attribute-based access control policy




### Configuration procedure

---

**Note**

- For detailed information about SSL configuration, refer to *SSL Configuration* in the *Security Volume*.
- For detailed information about HTTPS configuration, refer to *HTTP Server Configuration* in the *System Volume*.
- The PKI domain to be referenced by the SSL policy must be created in advance. For detailed configuration of the PKI domain, refer to Configure the PKI domain.

---

1) Configure the HTTPS server

# Configure the SSL policy for the HTTPS server to use.

```
<Switch> system-view
[Switch] ssl server-policy myssl
[Switch-ssl-server-policy-myssl] pki-domain 1
[Switch-ssl-server-policy-myssl] client-verify enable
[Switch-ssl-server-policy-myssl] quit
```

2) Configure the certificate attribute group

# Create certificate attribute group **mygroup1** and add two attribute rules. The first rule defines that the DN of the subject name includes the string **aabbcc**, and the second rule defines that the IP address of the certificate issuer is 10.0.0.1.

```
[Switch] pki certificate attribute-group mygroup1
[Switch-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
[Switch-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
[Switch-pki-cert-attribute-group-mygroup1] quit
```

# Create certificate attribute group **mygroup2** and add two attribute rules. The first rule defines that the FQDN of the alternative subject name does not include the string of **apple**, and the second rule defines that the DN of the certificate issuer name includes the string **aabbcc**.

```
[Switch] pki certificate attribute-group mygroup2
[Switch-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
[Switch-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
[Switch-pki-cert-attribute-group-mygroup2] quit
```

3) Configure the certificate attribute-based access control policy

# Create the certificate attribute-based access control policy of **myacp** and add two access control rules.

```
[Switch] pki certificate access-control-policy myacp
[Switch-pki-cert-acp-myacp] rule 1 deny mygroup1
[Switch-pki-cert-acp-myacp] rule 2 permit mygroup2
[Switch-pki-cert-acp-myacp] quit
```

4) Apply the SSL server policy and certificate attribute-based access control policy to HTTPS service and enable HTTPS service.

# Apply SSL server policy **myssl** to HTTPS service.

```
[Switch] ip https ssl-server-policy myssl
```

# Apply the certificate attribute-based access control policy of **myacp** to HTTPS service.

```
[Switch] ip https certificate access-control-policy myacp
```

# Enable HTTPS service.

```
[Switch] ip https enable
```

# Troubleshooting PKI

## Failed to Retrieve a CA Certificate

### Symptom

Failed to retrieve a CA certificate.

### Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- The system clock of the device is not synchronized with that of the CA.

### Solution

- Make sure that the network connection is physically proper.
- Check that the required commands are configured properly.
- Use the **ping** command to check that the RA server is reachable.
- Specify the authority for certificate request.
- Synchronize the system clock of the device with that of the CA.

## Failed to Request a Local Certificate

### Symptom

Failed to request a local certificate.

### Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No CA certificate has been retrieved.
- The current key pair has been bound to a certificate.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- Some required parameters of the entity DN are not configured.

### Solution

- Make sure that the network connection is physically proper.
- Retrieve a CA certificate.
- Regenerate a key pair.
- Specify a trusted CA.
- Use the **ping** command to check that the RA server is reachable.
- Specify the authority for certificate request.
- Configure the required entity DN parameters.

## Failed to Retrieve CRLs

### Symptom

Failed to retrieve CRLs.

### Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No CA certificate has been retrieved before you try to retrieve CRLs.
- The IP address of LDAP server is not configured.
- The CRL distribution URL is not configured.
- The LDAP server version is wrong.

### Solution

- Make sure that the network connection is physically proper.
- Retrieve a CA certificate.
- Specify the IP address of the LDAP server.
- Specify the CRL distribution URL.
- Re-configure the LDAP version.

# Table of Contents

# 1 SSL Configuration

When configuring SSL, go to these sections for information you are interested in:

- SSL Overview
- SSL Configuration Task List
- Displaying and Maintaining SSL
- Troubleshooting SSL

## SSL Overview

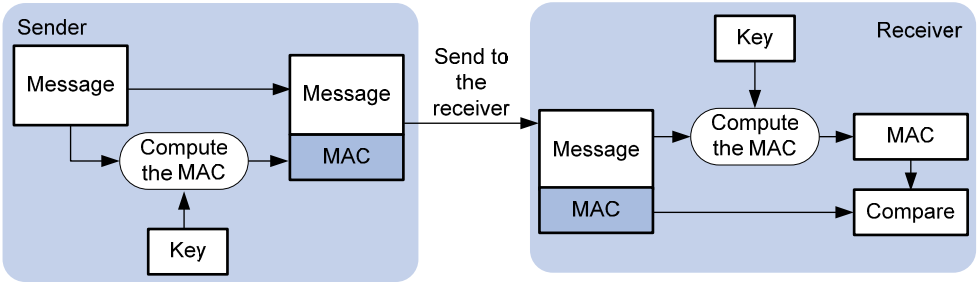
Secure Sockets Layer (SSL) is a security protocol providing secure connection service for TCP-based application layer protocols, for example, HTTP protocol. It is widely used in E-business and online bank fields to provide secure data transmission over the Internet.

### SSL Security Mechanism

SSL provides these security services:

- Confidentiality: SSL uses a symmetric encryption algorithm to encrypt data and uses the asymmetric key algorithm of Rivest, Shamir, and Adelman (RSA) to encrypt the key to be used by the symmetric encryption algorithm.
- Authentication: SSL supports certificate-based identity authentication of the server and client by using the digital signatures, with the authentication of the client being optional. The SSL server and client obtain certificates from a certificate authority (CA) through the Public Key Infrastructure (PKI).
- Reliability: SSL uses the key-based message authentication code (MAC) to verify message integrity. A MAC algorithm transforms a message of any length to a fixed-length message. Figure 1-1 illustrates how SSL uses a MAC algorithm to verify message integrity. With the key, the sender uses the MAC algorithm to compute the MAC value of a message. Then, the sender suffixes the MAC value to the message and sends the result to the receiver. The receiver uses the same key and MAC algorithm to compute the MAC value of the received message, and compares the locally computed MAC value with that received. If the two matches, the receiver considers the message intact; otherwise, the receiver considers that the message has been tampered with in transit and discards the message.

**Figure 1-1** Message integrity verification by a MAC algorithm



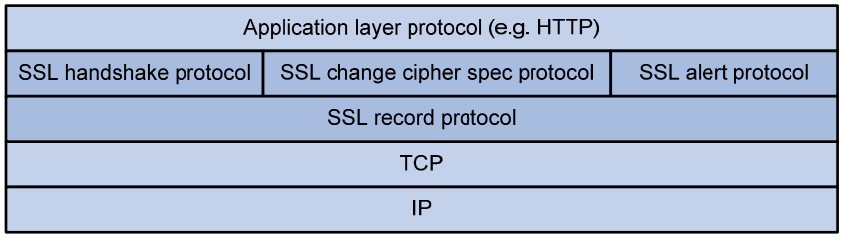
**Note**

- For details about symmetric key algorithms, asymmetric key algorithm RSA and digital signature, refer to *Public Key Configuration* in the *Security Volume*.
- For details about PKI, certificate, and CA, refer to *PKI Configuration* in the *Security Volume*.

## SSL Protocol Stack

As shown in Figure 1-2, the SSL protocol consists of two layers of protocols: the SSL record protocol at the lower layer and the SSL handshake protocol, change cipher spec protocol, and alert protocol at the upper layer.

**Figure 1-2** SSL protocol stack




- SSL handshake protocol: As a very important part of the SSL protocol stack, it is responsible for negotiating the cipher suite to be used during communication (including the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm), exchanging the key between the server and client, and implementing identity authentication of the server and client. Through the SSL handshake protocol, a session is established between a client and the server. A session consists of a set of parameters, including the session ID, peer certificate, cipher suite, and master secret.
- SSL change cipher spec protocol: Used for notification between a client and the server that the subsequent packets are to be protected and transmitted based on the newly negotiated cipher suite and key.
- SSL alert protocol: Allowing a client and the server to send alert messages to each other. An alert message contains the alert severity level and a description.
- SSL record protocol: Fragmenting and compressing data to be transmitted, calculating and adding MAC to the data, and encrypting the data before transmitting it to the peer end.

# SSL Configuration Task List

Different parameters are required on the SSL server and the SSL client.

Complete the following tasks to configure SSL:

| Task | Remarks |
|---|---|
| Configuring an SSL Server Policy | Required |
| Configuring an SSL Client Policy | Optional |

# Configuring an SSL Server Policy

An SSL server policy is a set of SSL parameters for a server to use when booting up. An SSL server policy takes effect only after it is associated with an application layer protocol, HTTP protocol, for example.

## Configuration Prerequisites

When configuring an SSL server policy, you need to specify the PKI domain to be used for obtaining the server side certificate. Therefore, before configuring an SSL server policy, you must configure a PKI domain. For details about PKI domain configuration, refer to *PKI Configuration* in the *Security Volume*.

## Configuration Procedure

Follow these steps to configure an SSL server policy:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an SSL server policy and enter its view | **ssl server-policy** *policy-name* | Required |
| Specify a PKI domain for the SSL server policy | **pki-domain** *domain-name* | Required<br>By default, no PKI domain is specified for an SSL server policy. |
| Specify the cipher suite(s) for the SSL server policy to support | **ciphersuite** [ **rsa_aes_128_cbc_sha** \| **rsa_des_cbc_sha** \| **rsa_rc4_128_md5** \| **rsa_rc4_128_sha** ] * | Optional<br>By default, an SSL server policy supports all cipher suites. |
| Set the handshake timeout time for the SSL server | **handshake timeout** *time* | Optional<br>3,600 seconds by default |
| Configure the SSL connection close mode | **close-mode wait** | Optional<br>Not wait by default |
| Set the maximum number of cached sessions and the caching timeout time | **session** { **cachesize** *size* \| **timeout** *time* } * | Optional<br>The defaults are as follows:<br>500 for the maximum number of cached sessions,<br>3600 seconds for the caching timeout time. |
| Enable certificate-based SSL client authentication | **client-verify enable** | Optional<br>Not enabled by default |

**Note**

- If you enable client authentication here, you must request a local certificate for the client.
- Currently, SSL mainly comes in these versions: SSL 2.0, SSL 3.0, and TLS 1.0, where TLS 1.0 corresponds to SSL 3.1. When the device acts as an SSL server, it can communicate with clients running SSL 3.0 or TLS 1.0, and can identify Hello packets from clients running SSL 2.0. If a client running SSL 2.0 also supports SSL 3.0 or TLS 1.0 (information about supported versions is carried in the packet that the client sends to the server), the server will notify the client to use SSL 3.0 or TLS 1.0 to communicate with the server.

## SSL Server Policy Configuration Example

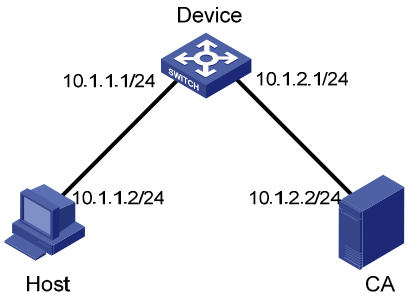
### Network requirements

- Device works as the HTTPS server.
- A host works as the client and accesses the HTTPS server through HTTP secured with SSL.
- A certificate authority (CA) issues a certificate to Device.

**Caution**

In this instance, Windows Server works as the CA and the Simple Certificate Enrollment Protocol (SCEP) plug-in is installed on the CA.

**Figure 1-3** Network diagram for SSL server policy configuration




### Configuration procedure

1) Request a certificate for Device

# Create a PKI entity named **en** and configure it.

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Create a PKI domain and configure it.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier ca1
[Device-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

# Create the local RSA key pairs.

```
[Device] public-key local create rsa
```

# Retrieve the CA certificate.

```
[Device] pki retrieval-certificate ca domain 1
```

# Request a local certificate.

```
[Device] pki request-certificate domain 1
```

2) Configure an SSL server policy

# Create an SSL server policy named **myssl**.

```
[Device] ssl server-policy myssl
```

# Specify the PKI domain for the SSL server policy as 1.

```
[Device-ssl-server-policy-myssl] pki-domain 1
```

# Enable client authentication.

```
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

3) Associate HTTPS service with the SSL server policy and enable HTTPS service

# Configure HTTPS service to use SSL server policy myssl.

```
[Device] ip https ssl-server-policy myssl
```

# Enable HTTPS service.

```
[Device] ip https enable
```

4) Verify your configuration

Launch IE on the host and enter https://10.1.1.1 in the address bar. You should be able to log in to Device and manage it.

---

 **Note**

- For details about PKI configuration commands, refer to *PKI Commands* in the *Security Volume*.
- For details about the **public-key local create rsa** command, refer to *Public Key Commands* in the *Security Volume*.
- For details about HTTPS, refer to *HTTP Configuration* in the *System Volume*.

---

## Configuring an SSL Client Policy

An SSL client policy is a set of SSL parameters for a client to use when connecting to the server. An SSL client policy takes effect only after it is associated with an application layer protocol.

### Configuration Prerequisites

If the SSL server is configured to authenticate the SSL client, when configuring the SSL client policy, you need to specify the PKI domain to be used for obtaining the certificate of the client. Therefore, before configuring an SSL client policy, you must configure a PKI domain. For details about PKI domain configuration, refer to *PKI Configuration* in the *Security Volume*.

### Configuration Procedure

Follow these steps to configure an SSL client policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an SSL client policy and enter its view | **ssl client-policy** *policy-name* | Required |
| Specify a PKI domain for the SSL client policy | **pki-domain** *domain-name* | Required<br>No PKI domain is configured by default. |
| Specify the preferred cipher suite for the SSL client policy | **prefer-cipher** { **rsa_aes_128_cbc_sha** \| **rsa_des_cbc_sha** \| **rsa_rc4_128_md5** \| **rsa_rc4_128_sha** } | Optional<br>**rsa_rc4_128_md5** by default |
| Specify the SSL protocol version for the SSL client policy | **version** { **ssl3.0** \| **tls1.0** } | Optional<br>TLS 1.0 by default |

**Note**

If you enable client authentication on the server, you must request a local certificate for the client.

## Displaying and Maintaining SSL

| To do… | Use the command… | Remarks |
|---|---|---|
| Display SSL server policy information | **display ssl server-policy** { *policy-name* \| **all** } | Available in any view |
| Display SSL client policy information | **display ssl client-policy** { *policy-name* \| **all** } | |

## Troubleshooting SSL

### SSL Handshake Failure

#### Symptom

As the SSL server, the device fails to handshake with the SSL client.

## Analysis

SSL handshake failure may result from the following causes:

- No SSL server certificate exists, or the certificate is not trusted.
- The server is expected to authenticate the client, but the SSL client has no certificate or the certificate is not trusted.
- The cipher suites used by the server and the client do not match.

## Solution

1) You can issue the **debugging ssl** command and view the debugging information to locate the problem:

- If the SSL server has no certificate, request one for it.
- If the server certificate cannot be trusted, install on the SSL client the root certificate of the CA that issues the local certificate to the SSL server, or let the server requests a certificate from the CA that the SSL client trusts.
- If the SSL server is configured to authenticate the client, but the certificate of the SSL client does not exist or cannot be trusted, request and install a certificate for the client.

2) You can use the **display ssl server-policy** command to view the cipher suite used by the SSL server policy. If the cipher suite used by the SSL server does not match that used by the client, use the **ciphersuite** command to modify the cipher suite of the SSL server.

# Table of Contents

# 1 Public Key Configuration

When configuring public keys, go to these sections for information you are interested in:

- Public Key Algorithm Overview
- Configuring the Local Asymmetric Key Pair
- Configuring the Public Key of a Peer
- Displaying and Maintaining Public Keys
- Public Key Configuration Examples

## Public Key Algorithm Overview

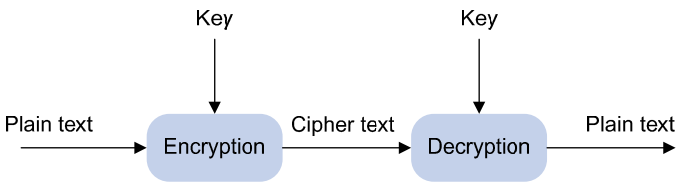
### Basic Concepts

- Algorithm: A set of transformation rules for encryption and decryption.
- Plain text: Information without being encrypted.
- Cipher text: Encrypted information.
- Key: A string of characters that controls the transformation between plain text and cipher text. It participates in both the encryption and decryption.

### Key Algorithm Types

As shown in Figure 1-1, the information is encrypted before being sent for confidentiality. The cipher text is transmitted in the network, and then is decrypted by the receiver to obtain the original pain text.

**Figure 1-1** Encryption and decryption




There are two types of key algorithms, based on whether the keys for encryption and decryption are the same:

- Symmetric key algorithm: The same key is used for both encryption and decryption. Commonly used symmetric key algorithms include AES and DES.
- Asymmetric key algorithm: Also called public key algorithm. Both ends have their own key pair, consisting of a private key and a public key. The private key is kept secret while the public key may be distributed widely. The private key cannot be practically derived from the public key. The information encrypted with the public key/private key can be decrypted only with the corresponding private key/public key.

### Asymmetric Key Algorithm Applications

Asymmetric key algorithms can be used for encryption and digital signature:

- Encryption: The information encrypted with a receiver's public key can be decrypted by the receiver possessing the corresponding private key. This is used to ensure confidentiality.
- Digital signature: The information encrypted with a sender's private key can be decrypted by anyone who has access to the sender's public key, thereby proving that the information is from the sender and has not been tampered with. For example, user 1 adds a signature to the data using the private key, and then sends the data to user 2. User 2 verifies the signature using the public key of user 1. If the signature is correct, the data is considered from user 1.

Revest-Shamir-Adleman Algorithm (RSA), and Digital Signature Algorithm (DSA) are all asymmetric key algorithms. RSA can be used for data encryption and signature, whereas DSA are used for signature only.

---

**Note**

Asymmetric key algorithms are usually used in digital signature applications for peer identity authentication because they involve complex calculations and are time-consuming; symmetric key algorithms are often used to encrypt data for security.

---

# Configuring the Local Asymmetric Key Pair

You can create and destroy a local asymmetric key pair, and export the host public key of a local asymmetric key pair.

## Creating an Asymmetric Key Pair

Follow these steps to create an asymmetric key pair:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a local DSA , or RSA key pairs | **public-key local create** { **dsa** \| **rsa** } | Required<br>By default, there is no such key pair. |

**Note**

- Configuration of the **public-key local create** command can survive a reboot.
- The **public-key local create rsa** command generates two key pairs: one server key pair and one host key pair. Each key pair consists of a public key and a private key.
- The length of an RSA key modulus is in the range 512 to 2048 bits. After entering the **public-key local create rsa** command, you will be required to specify the modulus length. For security, a modulus of at least 768 bits is recommended.
- The **public-key local create dsa** command generates only one key pair, that is, the host key pair.
- The length of a DSA key modulus is in the range 512 to 2048 bits. After entering the **public-key local create dsa** command, you will be required to specify the modulus length. For security, a modulus of at least 768 bits is recommended.

### Displaying or Exporting the Local RSA or DSA Host Public Key

You can display the local RSA or DSA host public key on the screen or export it to a specified file, so as to configure the local RSA or DSA host public key on the remote end.

Follow these steps to display or export the local RSA or DSA host public key:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Display the local RSA host public key on the screen in a specified format, or export it to a specified file | **public-key local export rsa** { **openssh** \| **ssh1** \| **ssh2** } [ *filename* ] | Select a command according to the type of the key to be exported. |
| Display the local DSA host public key on the screen in a specified format, or export it to a specified file | **public-key local export dsa** { **openssh** \| **ssh2** } [ *filename* ] | |

### Destroying an Asymmetric Key Pair

An asymmetric key pair may expire or leak. In this case, you need to destroy it and generate a new pair.

Follow these steps to destroy an asymmetric key pair:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Destroy an asymmetric key pair | **public-key local destroy** { **dsa** \| **rsa** } | Required |

## Configuring the Public Key of a Peer

To authenticate the remote host, you need to configure the RSA or DSA public key of that peer on the local host.

To configure the public key of the peer, you can:

- Configure it manually: You can input on or copy the public key of the peer to the local host. The copied public key must have not been converted and be in the distinguished encoding rules (DER) encoding format.
- Import it from the public key file: The system automatically converts the public key to a string coded using the PKCS (Public Key Cryptography Standards). Before importing the public key, you must upload the peer's public key file (in binary) to the local host through FTP or TFTP.

**Caution**

- You are recommended to configure the public key of the peer by importing it from a public key file.
- The device supports up to 20 host pubic keys of peers.

Follow these steps to configure the public key of a peer manually:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter public key view | **public-key peer** *keyname* | — |
| Enter public key code view | **public-key-code begin** | — |
| Configure a public key of the peer | Enter the key | Required<br>Spaces and carriage returns are allowed between characters. |
| Return to public key view | **public-key-code end** | —<br>When you exit public key code view, the system automatically saves the public key. |
| Return to system view | **peer-public-key end** | — |

Follow these steps to import the host public key of a peer from the public key file:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Import the host public key of a peer from the public key file | **public-key peer** *keyname*<br>**import sshkey** *filename* | Required |

## Displaying and Maintaining Public Keys

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the public keys of the local key pairs | **display public-key local** { **dsa** \| **rsa** } **public** | Available in any view |
| Display the public keys of the peers | **display public-key peer** [ **brief** \| **name** *publickey-name* ] | |

# Public Key Configuration Examples

## Configuring the Public Key of a Peer Manually

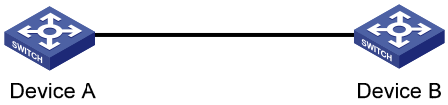
### Network requirements

Device A is authenticated by Device B when accessing Device B, so the public key of Device A should be configured on Device B in advance.

In this example:

- RSA is used.
- The host public key of Device A is configured manually on Device B.

**Figure 1-2** Network diagram for manually configuring the public key of a peer




### Configuration procedure

1) Configure Device A

# Create RSA key pairs on Device A.

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
++++++++
++++++++
```

# Display the public keys of the created RSA key pairs.

```
[DeviceA] display public-key local rsa public

=====================================================
Time of Key pair created: 09:50:06  2007/08/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

```
=====================================================
Time of Key pair created: 09:50:07  2007/08/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B0030680261009990 89E7AEE9802002D9EB2D0433B87BB6158E
35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E8
4B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

2) Configure Device B

# Configure the host public key of Device A on Device B. In public key code view, input the host public key of Device A. The host public key is the content of HOST_KEY displayed on Device A using the **display public-key local dsa public** command.

```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Public key view: return to System View with "peer-public-key end".
[DeviceB-pkey-public-key] public-key-code begin
Public key code view: return to last view with "public-key-code end".
[DeviceB-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100D90003F
A95F5A44A2A2CD3F814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A
9AB16C9E766BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326
470034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
[DeviceB-pkey-key-code] public-key-code end
[DeviceB-pkey-public-key] peer-public-key end
```

# Display the host public key of Device A saved on Device B.

```
[DeviceB] display public-key peer name devicea


=====================================
  Key Name  : devicea
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

## Importing the Public Key of a Peer from a Public Key File

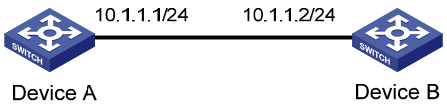
### Network requirements

Device A is authenticated when accessing Device B, so the public host public key of Device A should be configured on Device B in advance.

In this example:

- RSA is used.
- The host public key of Device A is imported from the public key file to Device B.

**Figure 1-3** Network diagram for importing the public key of a peer from a public key file




## Configurtion procedure

1) Create key pairs on Device A and export the host public key

# Create RSA key pairs on Device A.

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
++++++++
++++++++
```

# Display the public keys of the created RSA key pairs.

```
[DeviceA] display public-key local rsa public

=====================================================
Time of Key pair created: 09:50:06  2007/08/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001

=====================================================
Time of Key pair created: 09:50:07  2007/08/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B0030680261009990 89E7AEE9802002D9EB2D0433B87BB6158E
35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E8
4B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

# Export the RSA host public key to a file named **devicea.pub**.

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
```

```
[DeviceA] quit
```

2) Enable the FTP server function on Device B

# Enable the FTP server function, create an FTP user with the username **ftp** and password **123**.

```
<DeviceB> system-view
[DeviceB] ftp server enable
[DeviceB] local-user ftp
[DeviceB-luser-ftp] password simple 123
[DeviceB-luser-ftp] service-type ftp
[DeviceB-luser-ftp] authorization-attribute level 3
[DeviceB-luser-ftp] quit
```

3) Upload the public key file of Device A to Device B

# FTP the public key file **devicea.pub** to Device B.

```
<DeviceA> ftp 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
User(10.1.1.2:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
[ftp] put devicea.pub
227 Entering Passive Mode (10,1,1,2,5,148).
125 ASCII mode data connection already open, transfer starting for /devicea.pub.
226 Transfer complete.
FTP: 299 byte(s) sent in 0.189 second(s), 1.00Kbyte(s)/sec.
```

4) Import the host public key of Device A to Device B

# Import the host public key of Device A from the key file **devicea.pub** to Device B.

```
[DeviceB] public-key peer devicea import sshkey devicea.pub
```

# Display the host public key of Device A saved on Device B.

```
[DeviceB] display public-key peer name devicea

=====================================
  Key Name  : devicea
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

# Table of Contents

# 1 ACL Overview

In order to filter traffic, network devices use sets of rules, called access control lists (ACLs), to identify and handle packets.

When configuring ACLs, go to these chapters for information you are interested in:

- ACL Overview
- IPv4 ACL Configuration
- IPv6 ACL Configuration

---

**Note**

Unless otherwise stated, ACLs refer to both IPv4 ACLs and IPv6 ACLs throughout this document.

---

## Introduction to ACL

### Introduction

As network scale and network traffic are increasingly growing, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal users from accessing networks and to control network traffic and save network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

ACLs are sets of rules (or sets of permit or deny statements) that decide what packets can pass and what should be rejected based on matching criteria such as source MAC address, destination MAC address, source IP address, destination IP address, and port number.

### Application of ACLs on the Switch

The switch supports two ACL application modes:

- Hardware-based application: An ACL is assigned to a piece of hardware. For example, an ACL can be referenced by QoS for traffic classification. Note that when an ACL is referenced to implement QoS, the actions defined in the ACL rules, deny or permit, do not take effect; actions to be taken on packets matching the ACL depend on the traffic behavior definition in QoS. For details about traffic behavior, refer to the QoS part in *QoS Volume*.
- Software-based application: An ACL is referenced by a piece of upper layer software. For example, an ACL can be referenced to configure login user control behavior, thus controlling Telnet, SNMP and Web users. Note that when an ACL is reference by the upper layer software, actions to be taken on packets matching the ACL depend on those defined by the ACL rules. For details about login user control, refer to the part about login configuration in *System Volume*.

**Note**

- When an ACL is assigned to a piece of hardware and referenced by a QoS policy for traffic classification, the switch does not take action according to the traffic behavior definition on a packet that does not match the ACL.
- When an ACL is referenced by a piece of software to control Telnet, SNMP, and Web login users, the switch denies all packets that do not match the ACL.

# Introduction to IPv4 ACL

This section covers these topics:



## IPv4 ACL Classification

IPv4 ACLs, identified by ACL numbers, fall into three categories, as shown in Table 1-1.

**Table 1-1** IPv4 ACL categories

| Category | ACL number | Matching criteria |
|---|---|---|
| Basic IPv4 ACL | 2000 to 2999 | Source IP address |
| Advanced IPv4 ACL | 3000 to 3999 | Source IP address, destination IP address, protocol carried over IP, and other Layer 3 or Layer 4 protocol header information |
| Ethernet frame header ACL | 4000 to 4999 | Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority, and link layer protocol type |

## IPv4 ACL Naming

When creating an IPv4 ACL, you can specify a unique name for it. Afterwards, you can identify the ACL by its name.

An IPv4 ACL can have only one name. Whether to specify a name for an ACL is up to you. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.

**Note**

The name of an IPv4 ACL must be unique among IPv4 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.

## IPv4 ACL Match Order

An ACL may consist of multiple rules, which specify different matching criteria. These criteria may have overlapping or conflicting parts. The match order is for determining how packets should be matched against the rules.

Two match orders are available for IPv4 ACLs:

- **config**: Packets are compared against ACL rules in the order the rules are configured.
- **auto**: Packets are compared against ACL rules in the depth-first match order.

The term depth-first match has different meanings for different types of ACLs:

### Depth-first match for a basic IPv4 ACL

The following shows how your device performs depth-first match in a basic IPv4 ACL:

1) Sort rules by source IP address wildcard and compare packets against the rule configured with more zeros in the source IP address wildcard.
2) If two rules are present with the same number of zeros in their source IP address wildcards, compare packets against the rule configured first.

### Depth-first match for an advanced IPv4 ACL

The following shows how your device performs depth-first match in an advanced IPv4 ACL:

1) Look at the protocol carried over IP. A rule with no limit to the protocol type (that is, configured with the **ip** keyword) has the lowest precedence. Rules each of which has a single specified protocol type are of the same precedence level.
2) If the protocol types have the same precedence, look at the source IP address wildcards. Then, compare packets against the rule configured with more zeros in the source IP address wildcard.
3) If the numbers of zeros in the source IP address wildcards are the same, look at the destination IP address wildcards. Then, compare packets against the rule configured with more zeros in the destination IP address wildcard.
4) If the numbers of zeros in the destination IP address wildcards are the same, look at the Layer 4 port number ranges, namely the TCP/UDP port number ranges. Then compare packets against the rule configured with the smaller port number range.
5) If the port number ranges are the same, compare packets against the rule configured first.

### Depth-first match for an Ethernet frame header ACL

The following shows how your device performs depth-first match in an Ethernet frame header ACL:

1) Sort rules by source MAC address mask first and compare packets against the rule configured with more ones in the source MAC address mask.
2) If two rules are present with the same number of ones in their source MAC address masks, look at the destination MAC address masks. Then, compare packets against the rule configured with more ones in the destination MAC address mask.

3) If the numbers of ones in the destination MAC address masks are the same, compare packets against the one configured first.

The comparison of a packet against ACL rules stops immediately after a match is found. The packet is then processed as per the rule.

## IPv4 ACL Step

### Meaning of the step

The step defines the difference between two neighboring numbers that are automatically assigned to ACL rules by the device. For example, with a step of 5, rules are automatically numbered 0, 5, 10, 15, and so on. By default, the step is 5.

Whenever the step changes, the rules are renumbered, starting from 0. For example, if four rules are numbered 5, 10, 15, and 20 respectively, changing the step from 5 to 2 will cause the rules to be renumbered 0, 2, 4, and 6.

### Benefits of using the step

With the step and rule numbering/renumbering mechanism, you do not need to assign numbers to rules when defining them. The system will assign a newly defined rule a number that is the smallest multiple of the step bigger than the current biggest number. For example, with a step of five, if the biggest number is currently 28, the newly defined rule will get a number of 30. If the ACL has no rule defined already, the first defined rule will get a number of 0.

Another benefit of using the step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, and 15 in an ACL with a step of five, you can insert a rule numbered 1.

## Effective Period of an IPv4 ACL

You can control when a rule can take effect by referencing a time range in the rule.

A referenced time range can be one that has not been created yet. The rule, however, can take effect only after the time range is defined and becomes active.

## IP Fragments Filtering with IPv4 ACL

Traditional packet filtering performs match operation on, rather than all IP fragments, the first ones only. All subsequent non-first fragments are handled in the way the first fragments are handled. This causes security risk as attackers may fabricate non-first fragments to attack your network.

As for the configuration of a rule of an IPv4 ACL, the **fragment** keyword specifies that the rule applies to non-first fragment packets only, and does not apply to non-fragment packets or the first fragment packets. ACL rules that do not contain this keyword is applicable to both non-fragment packets and fragment packets.

# Introduction to IPv6 ACL

This section covers these topics:

- Effective Period of an IPv6 ACL

## IPv6 ACL Classification

IPv6 ACLs, identified by ACL numbers, fall into three categories, as shown in Table 1-2.

**Table 1-2** IPv6 ACL categories

| Category | ACL number | Matching criteria |
|---|---|---|
| Basic IPv6 ACL | 2000 to 2999 | Source IPv6 address |
| Advanced IPv6 ACL | 3000 to 3999 | Source IPv6 address, destination IPv6 address, protocol carried over IPv6, and other Layer 3 or Layer 4 protocol header information |

## IPv6 ACL Naming

When creating an IPv6 ACL, you can specify a unique name for it. Afterwards, you can identify the IPv6 ACL by its name.

An IPv6 ACL can have only one name. Whether to specify a name for an ACL is up to you. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.

---

**Note**

The name of an IPv6 ACL must be unique among IPv6 ACLs. However, an IPv6 ACL and an IPv4 ACL can share the same name.

---

## IPv6 ACL Match Order

Similar to IPv4 ACLs, an IPv6 ACL consists of multiple rules, each of which specifies different matching criteria. These criteria may have overlapping or conflicting parts. The match order is for determining how a packet should be matched against the rules.

Two match orders are available for IPv6 ACLs:

- **config**: Packets are compared against ACL rules in the order the rules are configured.
- **auto**: Packets are compared against ACL rules in the depth-first match order.

The term depth-first match has different meanings for different types of IPv6 ACLs:

### Depth-first match for a basic IPv6 ACL

The following shows how your device performs depth-first match in a basic IPv6 ACL:

1) Sort rules by source IPv6 address prefix first and compare packets against the rule configured with a longer prefix for the source IPv6 address.
2) In case of a tie, compare packets against the rule configured first.

### Depth-first match for an advanced IPv6 ACL

The following shows how your device performs depth-first match in an advanced IPv6 ACL:

1) Look at the protocol type field in the rules first. A rule with no limit to the protocol type (that is, configured with the **ipv6** keyword) has the lowest precedence. Rules each of which has a single specified protocol type are of the same precedence level. Compare packets against the rule with the highest precedence.
2) In case of a tie, look at the source IPv6 address prefixes. Then, compare packets against the rule configured with a longer prefix for the source IPv6 address.
3) If the prefix lengths for the source IPv6 addresses are the same, look at the destination IPv6 address prefixes. Then, compare packets against the rule configured with a longer prefix for the destination IPv6 address.
4) If the prefix lengths for the destination IPv6 addresses are the same, look at the Layer 4 port number ranges, namely the TCP/UDP port number ranges. Then compare packets against the rule configured with the smaller port number range.
5) If the port number ranges are the same, compare packets against the rule configured first.

The comparison of a packet against an ACL stops immediately after a match is found. The packet is then processed as per the rule.

## IPv6 ACL Step

Refer to IPv4 ACL Step.

## Effective Period of an IPv6 ACL

Refer to Effective Period of an IPv4 ACL.

# 2 IPv4 ACL Configuration

When configuring an IPv4 ACL, go to these sections for information you are interested in:



## Creating a Time Range

Two types of time ranges are available:

- Periodic time range, which recurs periodically on the day or days of the week.
- Absolute time range, which takes effect only in a period of time and does not recur.

### Configuration Procedure

Follow these steps to create a time range:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a time range | **time-range** *time-range-name* { *start-time* **to** *end-time days* [ **from** *time1 date1* ] [ **to** *time2 date2* ] \| **from** *time1 date1* [ **to** *time2 date2* ] \| **to** *time2 date2* } | Required |
| Display the configuration and status of one or all time ranges | **display time-range** { *time-range-name* \| **all** } | Optional<br>Available in any view |

You may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-range-name start-time* **to** *end-time days* command. A time range thus created recurs periodically on the day or days of the week. A periodic time range is active only when the system time falls within it.
- Absolute time range created using the **time-range** *time-range-name* { **from** *time1 date1* [ **to** *time2 date2* ] \| **to** *time2 date2* } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- Compound time range created using the **time-range** *time-range-name start-time* **to** *end-time days* { **from** *time1 date1* [ **to** *time2 date2* ] \| **to** *time2 date2* } command. A time range thus created recurs

on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.

- You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.
- If you do not specify the start time and date, the time range starts from the earliest time that the system supports, namely 00:00 01/01/1970. If you do not specify the end time and date, the time range ends at the latest time that the system supports, namely 24:00 12/31/2100.

### Configuration Example

# Create a time range that is active from 8:00 to 18:00 every working day.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

# Verify the configuration.

```
[Sysname] display time-range test
Current time is 22:17:42 1/5/2006 Thursday

Time-range : test ( Inactive )
 08:00 to 18:00 working-day
```

# Create an absolute time range from 15:00, Jan 28, 2006 to 15:00, Jan 28, 2008.

```
<Sysname> system-view
[Sysname] time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
[Sysname] display time-range test
Current time is 22:20:18 1/5/2006 Thursday

Time-range : test ( Inactive )
 from 15:00 1/28/2006 to 15:00 1/28/2008
```

## Configuring a Basic IPv4 ACL

Basic IPv4 ACLs match packets based on only source IP address. They are numbered from 2000 to 2999.

### Configuration Prerequisites

If you want to reference a time range in a rule, define it with the **time-range** command first.

## Configuration Procedure

Follow these steps to configure a basic IPv4 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic IPv4 ACL and enter its view | **acl number** *acl-number* [ **name** *acl-name* ] [ **match-order** { **auto** \| **config** } ] | Required<br>The default match order is **config**.<br>If you specify a name for an IPv4 ACL when creating the ACL, you can use the **acl name** *acl-name* command to enter the view of the ACL later. |
| Create or modify a rule | **rule** [ *rule-id* ] { **deny** \| **permit** } [ **fragment** \| **logging** \| **source** { *sour-addr sour-wildcard* \| **any** } \| **time-range** *time-range-name* ] * | Required<br>To create or modify multiple rules, repeat this step.<br>Note that the **logging** keyword is not supported if the ACL is to be referenced by a QoS policy for traffic classification. |
| Set the rule numbering step | **step** *step-value* | Optional<br>5 by default |
| Configure a description for the basic IPv4 ACL | **description** *text* | Optional<br>By default, a basic IPv4 ACL has no ACL description. |
| Configure a rule description | **rule** *rule-id* **comment** *text* | Optional<br>By default, an IPv4 ACL rule has no rule description. |

Note that:

- You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.
- You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
- When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

**Caution**

- You can modify the match order of an ACL with the **acl number** *acl-number* [ **name** *acl-name* ] **match-order** { **auto** | **config** } command, but only when the ACL does not contain any rules.
- The rule specified in the **rule comment** command must already exist.

## Configuration Example

# Configure IPv4 ACL 2000 to deny packets with source address 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

# Verify the configuration.

```
[Sysname-acl-basic-2000] display acl 2000
Basic ACL  2000, named -none-, 1 rule,
ACL's step is 5
 rule 0 deny source 1.1.1.1 0 (5 times matched)
```

# Configuring an Advanced IPv4 ACL

Advanced IPv4 ACLs match packets based on source IP address, destination IP address, protocol carried over IP, and other protocol header fields, such as the TCP/UDP source port number, TCP/UDP destination port number, TCP flag, ICMP message type, and ICMP message code.

In addition, advanced IPv4 ACLs allow you to filter packets based on three priority criteria: type of service (ToS), IP precedence, and differentiated services codepoint (DSCP) priority.

Advanced IPv4 ACLs are numbered in the range 3000 to 3999. Compared with basic IPv4 ACLs, they allow of more flexible and accurate filtering.

## Configuration Prerequisites

If you want to reference a time range in a rule, define it with the **time-range** command first.

## Configuration Procedure

Follow these steps to configure an advanced IPv4 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an advanced IPv4 ACL and enter its view | **acl number** *acl-number* [ **name** *acl-name* ] [ **match-order** { **auto** \| **config** } ] | Required<br>The default match order is **config**.<br>If you specify a name for an IPv4 ACL when creating the ACL, you can use the **acl name** *acl-name* command to enter the view of the ACL later. |
| Create or modify a rule | **rule** [ *rule-id* ] { **deny** \| **permit** } *protocol* [ { **ack** *ack-value* \| **fin** *fin-value* \| **psh** *psh-value* \| **rst** *rst-value* \| **syn** *syn-value* \| **urg** *urg-value* } * \| **destination** { *dest-addr dest-wildcard* \| **any** } \| **destination-port** *operator port1* [ *port2* ] \| **dscp** *dscp* \| **fragment** \| **icmp-type** { *icmp-type icmp-code* \| *icmp-message* } \| **logging** \| **precedence** *precedence* \| **reflective** \| **source** { *sour-addr sour-wildcard* \| **any** } \| **source-port** *operator port1* [ *port2* ] \| **time-range** *time-range-name* \| **tos** *tos* ] * | Required<br>To create or modify multiple rules, repeat this step.<br>Note that if the ACL is to be referenced by a QoS policy for traffic classification, the **logging** and **reflective** keywords are not supported and the *operator* argument cannot be **neq**. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the rule numbering step | **step** *step-value* | Optional<br>5 by default |
| Configure a description for the advanced IPv4 ACL | **description** *text* | Optional<br>By default, an advanced IPv4 ACL has no ACL description. |
| Configure a rule description | **rule** *rule-id* **comment** *text* | Optional<br>By default, an IPv4 ACL rule has no rule description. |

Note that:

- You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.
- You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
- When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

**Caution**

- You can modify the match order of an ACL with the **acl number** *acl-number* [ **name** *acl-name* ] **match-order** { **auto** | **config** } command, but only when the ACL does not contain any rules.
- The rule specified in the **rule comment** command must already exist.

## Configuration Example

# Configure IPv4 ACL 3000 to permit TCP packets with the destination port number of 80 from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
```

# Verify the configuration.

```
[Sysname-acl-adv-3000] display acl 3000
Advanced ACL  3000, named -none-, 1 rule,
ACL's step is 5
 rule  0  permit  tcp  source  129.9.0.0  0.0.255.255  destination  202.38.160.0  0.0.0.255
destination-port eq www (5 times matched)
```

# Configuring an Ethernet Frame Header ACL

Ethernet frame header ACLs match packets based on Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority (VLAN priority), and link layer protocol type. They are numbered in the range 4000 to 4999.

## Configuration Prerequisites

If you want to reference a time range in a rule, define it with the **time-range** command first.

## Configuration Procedure

Follow these steps to configure an Ethernet frame header ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an Ethernet frame header ACL and enter its view | **acl number** *acl-number* [ **name** *acl-name* ] [ **match-order** { **auto** \| **config** } ] | Required<br>The default match order is **config**.<br>If you specify a name for an IPv4 ACL when creating the ACL, you can use the **acl name** *acl-name* command to enter the view of the ACL later. |
| Create or modify a rule | **rule** [ *rule-id* ] { **deny** \| **permit** } [ **cos** *vlan-pri* \| **dest-mac** *dest-addr dest-mask* \| **lsap** *lsap-code lsap-wildcard* \| **source-mac** *sour-addr source-mask* \| **time-range** *time-range-name* \| **type** *type-code type-wildcard* ] * | Required<br>To create or modify multiple rules, repeat this step.<br>Note that the **lsap** keyword is not supported if the ACL is to be referenced by a QoS policy for traffic classification. |
| Set the rule numbering step | **step** *step-value* | Optional<br>5 by default |
| Configure a description for the Ethernet frame header ACL | **description** *text* | Optional<br>By default, an Ethernet frame header ACL has no ACL description. |
| Configure a rule description | **rule** *rule-id* **comment** *text* | Optional<br>By default, an Ethernet frame header ACL rule has no rule description. |

Note that:

- You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.
- You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
- When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

---

 **Caution**

- You can modify the match order of an ACL with the **acl number** *acl-number* [ **name** *acl-name* ] **match-order** { **auto** | **config** } command, but only when the ACL does not contain any rules.
- The rule specified in the **rule comment** command must already exist.

---

### Configuration Example

# Configure ACL 4000 to deny frames with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

# Verify the configuration.

```
[Sysname-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL  4000, named -none-, 1 rule,
ACL's step is 5
rule 0 deny cos excellent-effort(5 times matched)
```

## Copying an IPv4 ACL

This feature allows you to copy an existing IPv4 ACL to generate a new one, which is of the same type and has the same match order, rules, rule numbering step and descriptions as the source IPv4 ACL.

### Configuration Prerequisites

Make sure that the source IPv4 ACL exists while the destination IPv4 ACL does not.

### Configuration Procedure

Follow these steps to copy an IPv4 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Copy an existing IPv4 ACL to generate a new one of the same type | **acl copy** { *source-acl-number* \| **name** *source-acl-name* } **to** { *dest-acl-number* \| **name** *dest-acl-name* } | Required |

**Caution**

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The destination ACL does not take the name of the source IPv4 ACL.

# Displaying and Maintaining IPv4 ACLs

| To do... | Use the command… | Remarks |
|---|---|---|
| Display information about one or all IPv4 ACLs | **display acl** { *acl-number* \| **all** \| **name** *acl-name* } | Available in any view |
| Display information about ACL uses of a switch | **display acl resource** | Available in any view |
| Display the configuration and state of a specified or all time ranges | **display time-range** { *time-range-name* \| **all** } | Available in any view |
| Clear statistics about a specified or all IPv4 ACLs that are referenced by upper layer software | **reset acl counter** { *acl-number* \| **all** \| **name** *acl-name* } | Available in user view |

# IPv4 ACL Configuration Example

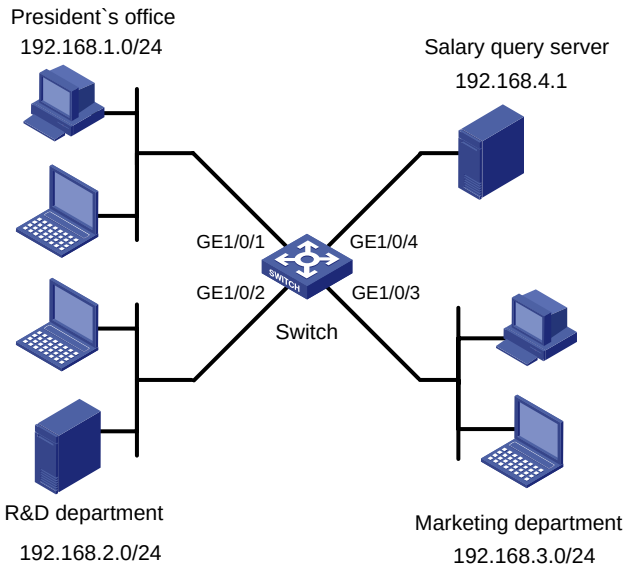
## Network Requirements

As shown in Figure 2-1, a company interconnects its departments through the switch.

Configure an ACL to deny access of all departments but the President's office to the salary query server during office hours (from 8:00 to 18:00) in working days.

## Network Diagram

**Figure 2-1** Network diagram for IPv4 ACL configuration



## Configuration Procedure

1) Create a time range for office hours

# Create a periodic time range spanning 8:00 to 18:00 in working days.

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

2) Define an ACL to control access to the salary query server

# Configure a rule to control access of the R&D Department to the salary query server.

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255 destination 192.168.4.1
0.0.0.0 time-range trname
[Switch-acl-adv-3000] quit
```

# Configure a rule to control access of the Marketing Department to the salary query server.

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule deny ip source 192.168.3.0 0.0.0.255 destination 192.168.4.1
0.0.0.0 time-range trname
[Switch-acl-adv-3001] quit
```

3) Apply the IPv4 ACL

# Configure class c_rd for packets matching IPv4 ACL 3000.

```
[Switch] traffic classifier c_rd
[Switch-classifier-c_rd] if-match acl 3000
[Switch-classifier-c_rd] quit
```

# Configure traffic behavior b_rd to deny matching packets.

```
[Switch] traffic behavior b_rd
[Switch-behavior-b_rd] filter deny
[Switch-behavior-b_rd] quit
```

# Configure class c_market for packets matching IPv4 ACL 3001.

```
[Switch] traffic classifier c_market
[Switch-classifier-c_market] if-match acl 3001
[Switch-classifier-c_market] quit
```

# Configure traffic behavior b_ market to deny matching packets.

```
[Switch] traffic behavior b_market
[Switch-behavior-b_market] filter deny
[Switch-behavior-b_market] quit
```

# Configure QoS policy p_rd to use traffic behavior b_rd for class c_rd.

```
[Switch] qos policy p_rd
[Switch-qospolicy-p_rd] classifier c_rd behavior b_rd
[Switch-qospolicy-p_rd] quit
```

# Configure QoS policy p_market to use traffic behavior b_market for class c_market.

```
[Switch] qos policy p_market
[Switch-qospolicy-p_market] classifier c_market behavior b_market
[Switch-qospolicy-p_market] quit
```

# Apply QoS policy p_rd to interface GigabitEthernet 1/0/2.

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy p_rd inbound
[Switch-GigabitEthernet1/0/2] quit
```

# Apply QoS policy p_market to interface GigabitEthernet 1/0/3.

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos apply policy p_market inbound
```

# 3 IPv6 ACL Configuration

When configuring IPv6 ACLs, go to these sections for information you are interested in:



## Creating a Time Range

Refer to Creating a Time Range.

## Configuring a Basic IPv6 ACL

Basic IPv6 ACLs match packets based on only source IPv6 address. They are numbered in the range 2000 to 2999.

### Configuration Prerequisites

If you want to reference a time range in a rule, define it with the **time-range** command first.

### Configuration Procedure

Follow these steps to configure an IPv6 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic IPv6 ACL view and enter its view | **acl ipv6 number** *acl6-number* [ **name** *acl6-name* ] [ **match-order** { **auto** \| **config** } ] | Required<br>The default match order is **config**.<br>If you specify a name for an IPv6 ACL when creating the ACL, you can use the **acl ipv6 name** *acl6-name* command to enter the view of the ACL later. |
| Create or modify a rule | **rule** [ *rule-id* ] { **deny** \| **permit** } [ **fragment** \| **logging** \| **source** { *ipv6-address prefix-length* \| *ipv6-address/prefix-length* \| **any** } \| **time-range** *time-range-name* ] * | Required<br>To create or modify multiple rules, repeat this step.<br>Note that the **logging** and **fragment** keywords are not supported if the ACL is to be referenced by a QoS policy for traffic classification. |
| Set the rule numbering step | **step** *step-value* | Optional<br>5 by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure a description for the basic IPv6 ACL | **description** *text* | Optional<br>By default, a basic IPv6 ACL has no ACL description. |
| Configure a rule description | **rule** *rule-id* **comment** *text* | Optional<br>By default, an IPv6 ACL rule has no rule description. |

Note that:

- You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.
- You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.
- When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

**Caution**

- You can modify the match order of an IPv6 ACL with the **acl ipv6 number** *acl6-number* [ **name** *acl6-name* ] **match-order** { **auto** | **config** } command, but only when the ACL does not contain any rules.
- The rule specified in the **rule comment** command must already exist.

### Configuration Example

# Configure IPv6 ACL 2000 to permit IPv6 packets with the source address of 2030:5060::9050/64 and deny IPv6 packets with the source address of fe80:5060::8050/96.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule deny source fe80:5060::8050/96
```

# Verify the configuration.

```
[Sysname-acl6-basic-2000] display acl ipv6 2000
 Basic IPv6 ACL  2000, named -none-, 2 rules,
 ACL's step is 5
 rule 0 permit source 2030:5060::9050/64 (4 times matched)
 rule 5 deny source FE80:5060::8050/96 (5 times matched)
```

## Configuring an Advanced IPv6 ACL

Advanced IPv6 ACLs match packets based on the source IPv6 address, destination IPv6 address, protocol carried over IPv6, and other protocol header fields such as the TCP/UDP source port number, TCP/UDP destination port number, ICMP message type, and ICMP message code.

Advanced IPv6 ACLs are numbered in the range 3000 to 3999. Compared with basic IPv6 ACLs, they allow of more flexible and accurate filtering.

## Configuration Prerequisites

If you want to reference a time range in a rule, define it with the **time-range** command first.

## Configuration Procedure

Follow these steps to configure an advanced IPv6 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an advanced IPv6 ACL and enter its view | **acl ipv6 number** *acl6-number* [ **name** *acl6-name* ] [ **match-order** { **auto** \| **config** } ] | Required<br>The default match order is **config**.<br>If you specify a name for an IPv6 ACL when creating the ACL, you can use the **acl ipv6 name** *acl6-name* command to enter the view of the ACL later. |
| Create or modify a rule | **rule** [ *rule-id* ] { **deny** \| **permit** } *protocol* [ { **ack** *ack-value* \| **fin** *fin-value* \| **psh** *psh-value* \| **rst** *rst-value* \| **syn** *syn-value* \| **urg** *urg-value* } * \| **destination** { *dest dest-prefix* \| *dest/dest-prefix* \| **any** } \| **destination-port** *operator port1* [ *port2* ] \| **dscp** *dscp* \| **fragment** \| **icmpv6-type** { *icmpv6-type icmpv6-code* \| *icmpv6-message* } \| **logging** \| **source** { *source source-prefix* \| *source/source-prefix* **\| any** } \| **source-port** *operator port1* [ *port2* ] \| **time-range** *time-range-name* ] * | Required<br>To create or modify multiple rules, repeat this step.<br>Note that if the ACL is to be referenced by a QoS policy for traffic classification, the **logging** and **fragment** keywords are not supported and the *operator* argument cannot be:<br>• **neq**, if the policy is for the inbound traffic,<br>• **gt**, **lt**, **neq** or **range**, if the policy is for the outbound traffic. |
| Set the rule numbering step | **step** *step-value* | Optional<br>5 by default |
| Configure a description for the advanced IPv6 ACL | **description** *text* | Optional<br>By default, an advanced IPv6 ACL has no ACL description. |
| Configure a rule description | **rule** *rule-id* **comment** *text* | Optional<br>By default, an IPv6 ACL rule has no rule description. |

Note that:

- You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.
- You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

- When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

---

**Caution**

- You can modify the match order of an IPv6 ACL with the **acl ipv6 number** *acl6-number* [ **name** *acl6-name* ] **match-order** { **auto** | **config** } command, but only when the ACL does not contain any rules.
- The rule specified in the **rule comment** command must already exist.

---

### Configuration Example

# Configure IPv6 ACL 3000 to permit TCP packets with the source address of 2030:5060::9050/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

# Verify the configuration.

```
[Sysname-acl6-adv-3000] display acl ipv6 3000
 Advanced IPv6 ACL  3000, named -none-, 1 rule,
 ACL's step is 5
 rule 0 permit tcp source 2030:5060::9050/64 (5 times matched)
```

## Copying an IPv6 ACL

This feature allows you to copy an existing IPv6 ACL to generate a new one, which is of the same type and has the same match order, rules, rule numbering step, and descriptions as the source IPv6 ACL.

### Configuration Prerequisites

Make sure that the source IPv6 ACL exists while the destination IPv6 ACL does not.

### Configuration Procedure

Follow these steps to copy an IPv6 ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Copy an existing IPv6 ACL to generate a new one of the same type | **acl ipv6 copy** { *source-acl6-number* \| **name** *source-acl6-name* } **to** { *dest-acl6-number* \| **name** *dest-acl6-name* } | Required |

**Caution**

- The source IPv6 ACL and the destination IPv6 ACL must be of the same type.
- The destination ACL does not take the name of the source IPv6 ACL.

# Displaying and Maintaining IPv6 ACLs

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about one or all IPv6 ACLs | **display acl ipv6** { *acl6-number* \| **all** \| **name** *acl6-name* } | Available in any view |
| Display information about ACL uses of a switch | **display acl resource** | Available in any view |
| Display the configuration and status on time range | **display time-range** { *time-range-name* \| **all** } | Available in any view |
| Clear statistics about a specified or all IPv6 ACLs that are referenced by upper layer software | **reset acl ipv6 counter** { *acl6-number* \| **all** \| **name** *acl6-name* } | Available in user view |

# IPv6 ACL Configuration Example

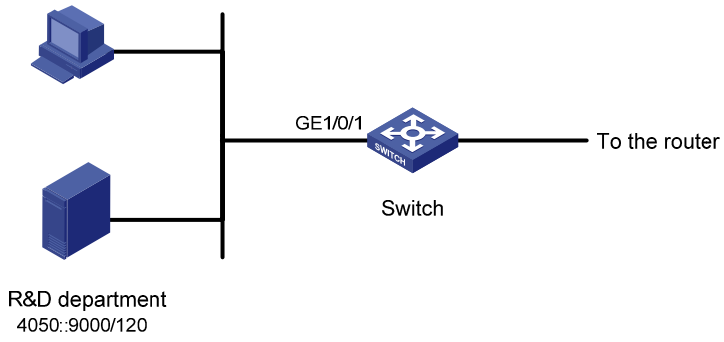
## Network Requirements

As shown in Figure 3-1, a company interconnects its departments through the switch.

Configure an ACL to deny access of the R&D department to external networks.

## Network Diagram

**Figure 3-1** Network diagram for IPv6 ACL configuration




## Configuration Procedure

# Create an IPv6 ACL 2000.

```
<Switch> system-view
[Switch] acl ipv6 number 2000
[Switch-acl6-basic-2000] rule deny source 4050::9000/120
```

```
[Switch-acl6-basic-2000] quit
```

# Configure class c_rd for packets matching IPv6 ACL 2000.

```
[Switch] traffic classifier c_rd
[Switch-classifier-c_rd] if-match acl ipv6 2000
[Switch-classifier-c_rd] quit
```

# Configure traffic behavior b_rd to deny matching packets.

```
[Switch] traffic behavior b_rd
[Switch-behavior-b_rd] filter deny
[Switch-behavior-b_rd] quit
```

# Configure QoS policy p_rd to use traffic behavior b_rd for class c_rd.

```
[Switch] qos policy p_rd
[Switch-qospolicy-p_rd] classifier c_rd behavior b_rd
[Switch-qospolicy-p_rd] quit
```

# Apply QoS policy p_rd to interface GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy p_rd inbound
```

# System Volume Organization

## Manual Version

6W100-20090210

## Product Version

V05.02.00

## Organization

The System Volume is organized as follows:

| Features | Description |
|---|---|
| Login | Upon logging into a device, you can configure user interface properties and manage the system conveniently. This document describes:<br>• How to log in to your Ethernet switch<br>• Introduction to the user interface and common configurations<br>• Logging In Through the Console Port<br>• Logging In Through Telnet<br>• Logging in Through Web-based Network Management System<br>• Logging In Through NMS<br>• Specifying Source IP address/Interface for Telnet Packets<br>• Controlling Login Users |
| Basic System Configuration | Basic system configuration involves the configuration of device name, system clock, welcome message, user privilege levels and so on. This document describes:<br>• Configuration display<br>• Basic configurations<br>• CLI features |

| Features | Description |
| --- | --- |
| Device Management | Through the device management function, you can view the current condition of your device and configure running parameters. This document describes:<br>• Device management overview<br>• Rebooting a device<br>• Configuring the scheduled automatic execution function<br>• Specifying a file for the next device boot<br>• Upgrading Boot ROM<br>• Configuring a detection interval<br>• Configuring temperature alarm thresholds for a board<br>• Clearing the 16-bit interface indexes not used in the current system<br>• Configuring the system load sharing function<br>• Configuring the traffic forwarding mode of SRPUs<br>• Configuring the working mode of EA LPUs<br>• Enabling the port down function globally<br>• Enabling expansion memory data recovery function on a board<br>• Identifying and diagnosing pluggable transceivers |
| File System Management | A major function of the file system is to manage storage devices, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file. This document describes:<br>• File system management<br>• Configuration File Management<br>• FTP configuration<br>• TFTP configuration |
| HTTP | Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. This document describes:<br>• HTTP Configuration<br>• HTTPS Configuration |
| SNMP | Simple network management protocol (SNMP) offers a framework to monitor network devices through TCP/IP protocol suite. This document describes:<br>• SNMP overview<br>• Basic SNMP function configuration<br>• SNMP log configuration<br>• Trap configuration<br>• MIB style configuration |
| RMON | RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. This document describes:<br>• RMON overview<br>• RMON configuration |

| Features | Description |
| --- | --- |
| MAC Address Table Management | A switch maintains a MAC address table for fast forwarding packets. This document describes:<br>• MAC address table overview<br>• Configuring MAC Address Entries<br>• Configuring the Aging Timer for Dynamic MAC Address Entries<br>• Configuring the MAC Learning Limit<br>• Configuring MAC Information |
| System Maintenance and Debugging | For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors. This document describes:<br>• Maintenance and debugging overview<br>• Maintenance and debugging configuration |
| Information Center | As the system information hub, Information Center classifies and manages all types of system information. This document describes:<br>• Information Center Overview<br>• Setting to Output System Information to the Console<br>• Setting to Output System Information to a Monitor Terminal<br>• Setting to Output System Information to a Log Host<br>• Setting to Output System Information to the Trap Buffer<br>• Setting to Output System Information to the Log Buffer<br>• Setting to Output System Information to the SNMP Module<br>• Configuring Synchronous Information Output<br>• Disabling a Port from Generating Link Up/Down Logging Information |
| PoE | The Power over Ethernet (PoE) feature enables the power sourcing equipment (PSE) to feed powered devices (PDs) from Ethernet ports through twisted pair cables. This document describes:<br>• PoE overview<br>• Configuring the PoE Interface<br>• Configuring PoE power management<br>• Configuring the PoE monitoring function<br>• Online upgrading the PSE processing software<br>• Configuring a PD Disconnection Detection Mode<br>• Enabling the PSE to detect nonstandard PDs |
| Track | The track module is used to implement collaboration between different modules through established collaboration objects. The detection modules trigger the application modules to perform certain operations through the track module. This document describes:<br>• Track Overview<br>• Configuring Collaboration Between the Track Module and the Detection Modules<br>• Configuring Collaboration Between the Track Module and the Application Modules |

| Features | Description |
| --- | --- |
| NQA | NQA analyzes network performance, services and service quality by sending test packets to provide you with network performance and service quality parameters. This document describes:<br>• NQA Overview<br>• Configuring the NQA Server<br>• Enabling the NQA Client<br>• Creating an NQA Test Group<br>• Configuring an NQA Test Group<br>• Configuring the Collaboration Function<br>• Configuring Trap Delivery<br>• Configuring the NQA Statistics Function<br>• Configuring Optional Parameters Common to an NQA Test Group<br>• Scheduling an NQA Test Group |
| NTP | Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network. This document describes:<br>• NTP overview<br>• Configuring the Operation Modes of NTP<br>• Configuring Optional Parameters of NTP<br>• Configuring Access-Control Rights<br>• Configuring NTP Authentication |
| Hotfix | Hotfix is a fast, cost-effective method to fix software defects of the device without interrupting the running services. This document describes:<br>• Hotfix Overview<br>• One-Step Patch Installation<br>• Step-by-Step Patch Installation<br>• Step-by-Step Patch Uninstallation<br>• One-Step Patch Uninstallation |
| Cluster Management | A cluster is a group of network devices. Cluster management is to implement management of large numbers of distributed network devices. This document describes:<br>• Cluster Management Overview<br>• Configuring the Management Device<br>• Configuring the Member Devices<br>• Configuring Access Between the Management Device and Its Member Devices<br>• Adding a Candidate Device to a Cluster<br>• Configuring Advanced Cluster Functions |
| Stack Management | A stack is a set of network devices. Administrators can group multiple network devices into a stack and manage them as a whole. Therefore, stack management can help reduce customer investments and simplify network management. This document describes:<br>• Stack Configuration Overview<br>• Configuring the Master Device of a Stack<br>• Configuring Stack Ports of a Slave Device<br>• Logging In to the CLI of a Slave from the Master |

| Features | Description |
| --- | --- |
| Automatic Configuration | Automatic configuration enables a device to automatically obtain and execute the configuration file when it starts up without loading the configuration file. This document describes:<br>• Introduction to Automatic Configuration<br>• Typical Networking of Automatic Configuration<br>• How Automatic Configuration Works |

# Table of Contents

# 1 Logging In to an Ethernet Switch

When logging in to an Ethernet switch, go to these sections for information you are interested in:



## Logging In to an Ethernet Switch

You can log in to an 3Com Switch 4500G in one of the following ways:

- Logging in locally through the Console port
- Telnetting locally or remotely to an Ethernet port
- Logging in through NMS (network management station)

## Introduction to User Interface

### Supported User Interfaces

3Com Switch 4500G supports two types of user interfaces: AUX and VTY.

**Table 1-1** Description on user interface

| User interface | Applicable user | Port used | Description |
|---|---|---|---|
| AUX | Users logging in through the Console port | Console port | Each switch can accommodate one AUX user. |
| VTY | Telnet users and SSH users | Ethernet port | Each switch can accommodate up to five VTY users. |

**Note**

As the AUX port and the Console port of a 3Com Switch 4500G are the same one, you will be in the AUX user interface if you log in through this port.

### User Interface Number

Two kinds of user interface index exist: absolute user interface index and relative user interface index.

1) The absolute user interface indexes are as follows:

- AUX user interface: 0
- VTY user interfaces: Numbered after AUX user interfaces and increases in the step of 1

2) A relative user interface index can be obtained by appending a number to the identifier of a user interface type. It is generated by user interface type. The relative user interface indexes are as follows:

- AUX user interface: AUX 0
- VTY user interfaces: VTY 0, VTY 1, VTY 2, and so on.

## Common User Interface Configuration

Follow these steps to perform common user interface configuration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Lock the current user interface | **lock** | Optional<br>Execute this command in user view.<br>A user interface is not locked by default. |
| Specify to send messages to all user interfaces/a specified user interface | **send** { **all** \| *number* \| *type number* } | Optional<br>Execute this command in user view. |
| Disconnect a specified user interface | **free user-interface** [ *type* ] *number* | Optional<br>Execute this command in user view. |
| Enter system view | **system-view** | — |
| Set the banner | **header** { **incoming** \| **legal** \| **login** \| **shell** \| **motd** } *text* | Optional |
| Set a system name for the switch | **sysname** *string* | Optional<br>Default is 4500G |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Define a shortcut key for aborting tasks | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Set the history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
| Set the timeout time for the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

| To do… | Use the command… | Remarks |
| --- | --- | --- |
| Set the maximum number of lines the screen can contain | screen-length screen-length | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the screen-length 0 command to disable the function to display information in pages. |
| Make terminal services available | shell | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the display type of a terminal | terminal type { ansi \| vt100 } | Optional<br>By default, the terminal display type is ANSI. The device must use the same type of display as the terminal. If the terminal uses VT 100, the device should also use VT 100. |
| Display the information about the current user interface/all user interfaces | **display users** [ **all** ] | You can execute this command in any view. |
| Display the physical attributes and configuration of the current/a specified user interface | **display user-interface** [ *type number* \| *number* ] [ **summary** ] | You can execute this command in any view. |

# 2 Logging In Through the Console Port

When logging in through the Console port, go to these sections for information you are interested in:



## Introduction

To log in through the Console port is the most common way to log in to a switch. It is also the prerequisite to configure other login methods. By default, you can log in to an 3Com Switch 4500G through its Console port only.

To log in to an Ethernet switch through its Console port, the related configuration of the user terminal must be in accordance with that of the Console port.

Table 2-1 lists the default settings of a Console port.

**Table 2-1** The default settings of a Console port

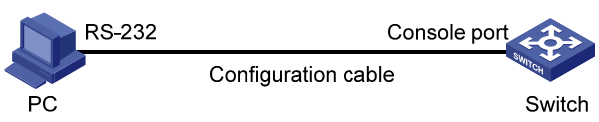
| Setting | Default |
|---|---|
| Baud rate | 19,200 bps |
| Flow control | Off |
| Check mode | No check bit |
| Stop bits | 1 |
| Data bits | 8 |

After logging in to a switch, you can perform configuration for AUX users. Refer to Console Port Login Configuration for details.

## Setting Up the Connection to the Console Port

- Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 2-1.

**Figure 2-1** Diagram for setting the connection to the Console port



- If you use a PC to connect to the Console port, launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X/Windows 2000/Windows XP) and perform the configuration shown in Figure 2-2 through Figure 2-4 for the connection to be created. Normally, the parameters of a terminal are configured as those listed in Table 2-1.

**Figure 2-2** Create a connection

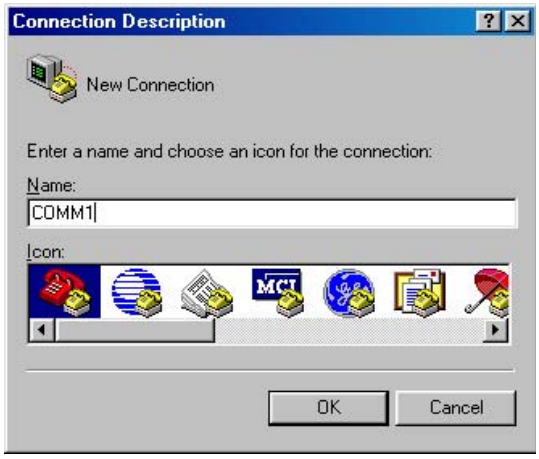
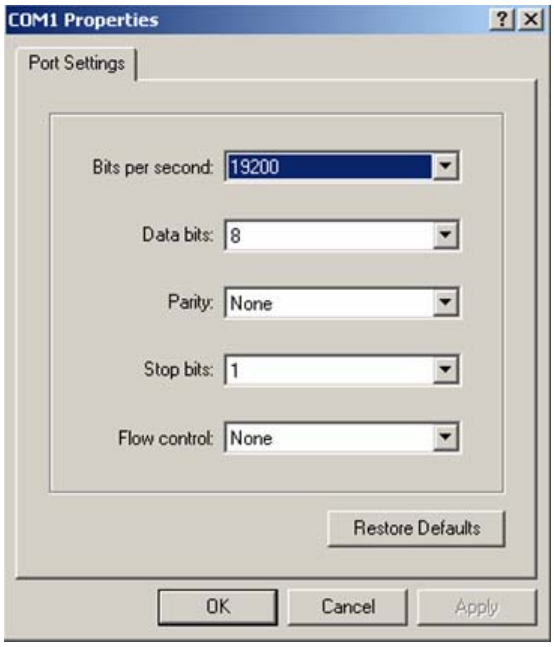



**Figure 2-3** Specify the port used to establish the connection

**Figure 2-4** Set port parameters terminal window




- Turn on the switch. The user will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as <4500G>) appears after the user presses the Enter key.

**Note**

The username is " admin " and none of the password.

- You can then configure the switch or check the information about the switch by executing commands. You can also acquire help by type the ? character. Refer to the following chapters for information about the commands.

# Console Port Login Configuration

## Common Configuration

Table 2-2 lists the common configuration of Console port login.

**Table 2-2** Common configuration of Console port login

| Configuration | | Description |
|---|---|---|
| Console port configuration | Baud rate | Optional<br>The default baud rate is 19,200 bps. |

| Configuration | | Description |
|---|---|---|
| | Check mode | Optional<br>By default, the check mode of the Console port is set to “none”, which means no check bit. |
| | Stop bits | Optional<br>The default stop bits of a Console port is 1. |
| | Data bits | Optional<br>The default data bits of a Console port is 8. |
| | Flow control | Optional<br>The default is **none**, which disables flow control. |
| AUX user interface configuration | Configure the command level available to the users logging in to the AUX user interface | Optional<br>By default, commands of level 3 are available to the users logging in to the AUX user interface. |
| Terminal configuration | Define a shortcut key for aborting tasks | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| | Define a shortcut key for starting terminal sessions | Optional<br>By default, pressing Enter key starts the terminal session. |
| | Make terminal services available | Optional<br>By default, terminal services are available in all user interfaces |
| | Set the maximum number of lines the screen can contain | Optional<br>By default, the screen can contain up to 24 lines. |
| | Set history command buffer size | Optional<br>By default, the history command buffer can contain up to 10 commands. |
| | Set the timeout time of a user interface | Optional<br>The default timeout time is 10 minutes. |

**Caution**

Changing of Console port configuration terminates the connection to the Console port. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly. Refer to Setting Up the Connection to the Console Port for details.

## Console Port Login Configurations for Different Authentication Modes

Table 2-3 lists Console port login configurations for different authentication modes.

**Table 2-3** Console port login configurations for different authentication modes

| Authentication mode | Console port login configuration | | Description |
|---|---|---|---|
| None | Perform common configuration | Perform common configuration for Console port login | Optional<br>Refer to Common Configuration for details. |
| Password | Configure the password | Configure the password for local authentication | Required |
| | Perform common configuration | Perform common configuration for Console port login | Optional<br>Refer to Common Configuration for details. |
| Scheme | Specify to perform local authentication or RADIUS authentication | AAA configuration specifies whether to perform local authentication or RADIUS authentication | Optional<br>Local authentication is performed by default.<br>Refer to the AAA Configuration in the Security Volume for details. |
| | Configure user name and password | Configure user names and passwords for local/remote users | Required<br>• The user name and password of a local user are configured on the switch.<br>• The user name and password of a remote user are configured on the RADIUS server. Refer to user manual of RADIUS server for details. |
| | Manage AUX users | Set service type for AUX users | Required |
| | Perform common configuration | Perform common configuration for Console port login | Optional<br>Refer to Common Configuration for details. |

**Note**

Changes of the authentication mode of Console port login will not take effect unless you exit and enter again the CLI.

# Console Port Login Configuration with Authentication Mode Being None

## Configuration Procedure

Follow these steps to perform Console port login configuration (with authentication mode being **none**):

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter AUX user interface view | | **user-interface aux** 0 | — |
| Configure not to authenticate users | | **authentication-mode none** | Required<br>By default, users logging in through the Console port is scheme authenticated. |
| Configure the Console port | Set the baud rate | **speed** speed-value | Optional<br>The default baud rate of an AUX port (also the Console port) is 19,200 bps. |
| | Set the check mode | **parity** { **even** \| **mark** \| **none** \| **odd** \| **space** } | Optional<br>By default, the check mode of a Console port is set to **none**, that is, no check bit. |
| | Set the stop bits | **stopbits** { **1** \| **1.5** \| **2** } | Optional<br>The stop bits of a Console port is 1. |
| | Set the data bits | **databits** { **5** \| **6** \| **7** \| **8** } | Optional<br>The default data bits of a Console port is 8. |
| Configure the command level available to users logging in to the user interface | | **user privilege level** *level* | Optional<br>By default, commands of level 3 are available to users logging in to the AUX user interface. |
| Define a shortcut key for starting terminal sessions | | **activation-key** *character* | Optional<br>By default, pressing Enter key starts the terminal session. |
| Define a shortcut key for aborting tasks | | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available | | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set the history command buffer size | | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the timeout time for the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that if you configure not to authenticate the users, the command level available to users logging in to a switch depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in the following table.

**Table 2-4** Determine the command level (A)

| Scenario | | | Command level |
|---|---|---|---|
| **Authentication mode** | **User type** | **Command** | |
| None (authentication-mode none) | Users logging in through Console ports | The user privilege level *level* command not executed | Level 3 |
| | | The user privilege level *level* command already executed | Determined by the *level* argument |

## Configuration Example

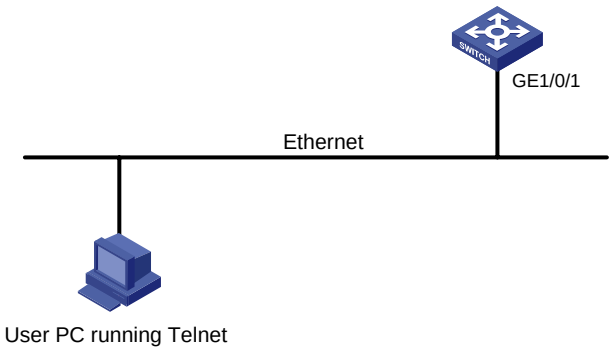
### Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the console user at the following aspects.

- The user is not authenticated when logging in through the Console port.
- Commands of level 2 are available to user logging in to the AUX user interface.
- The baud rate of the Console port is 19200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

### Network diagram

**Figure 2-5** Network diagram for AUX user interface configuration (with the authentication mode being **none**)




### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

# Specify not to authenticate the user logging in through the Console port.

```
[Sysname-ui-aux0] authentication-mode none
```

# Specify commands of level 2 are available to the user logging in to the AUX user interface.

```
[Sysname-ui-aux0] user privilege level 2
```

# Set the baud rate of the Console port to 19200 bps.

```
[Sysname-ui-aux0] speed 19200
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

# Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, to ensure a successful login, the console user needs to change the corresponding configuration of the terminal emulation program running on the PC, to make the configuration consistent with that on the switch. Refer to Setting Up the Connection to the Console Port for details.

# Console Port Login Configuration with Authentication Mode Being Password

## Configuration Procedure

Follow these steps to perform Console port login configuration (with authentication mode being **password**):

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter AUX user interface view | | **user-interface aux** 0 | — |
| Configure to authenticate users using the local password | | **authentication-mode password** | Required<br>By default, users logging in through the Console port and Telnet need to pass the scheme authentication. |
| Set the local password | | **set authentication password** { **cipher** \| **simple** } *password* | Required |
| Configure the Console port | Set the baud rate | **speed** speed-value | Optional<br>The default baud rate of an AUX port (also the Console port) is 19,200 bps. |
| | Set the check mode | **parity** { **even** \| **mark** \| **none** \| **odd** \| **space** } | Optional<br>By default, the check mode of a Console port is set to **none**, that is, no check bit. |
| | Set the stop bits | **stopbits** { **1** \| **1.5** \| **2** } | Optional<br>The default stop bits of a Console port is 1. |
| | Set the data bits | **databits** { **5** \| **6** \| **7** \| **8** } | Optional<br>The default data bits of a Console port is 8. |
| Configure the command level available to users logging in to the user interface | | **user privilege level** *level* | Optional<br>By default, commands of level 3 are available to users logging in to the AUX user interface. |
| Define a shortcut key for starting terminal sessions | | **activation-key** *character* | Optional<br>By default, pressing Enter key starts the terminal session. |
| Define a shortcut key for aborting tasks | | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available to the user interface | | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set history command buffer size | | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the timeout time for the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that if you configure to authenticate the users in the password mode, the command level available to users logging in to a switch depends on both the **authentication-mode password** and the **user privilege level** *level* command, as listed in the following table.

**Table 2-5** Determine the command level (B)

| Scenario | | | Command level |
|---|---|---|---|
| **Authentication mode** | **User type** | **Command** | |
| Local authentication (authentication-mode password) | Users logging in to the AUX user interface | The user privilege level *level* command not executed | Level 3 |
| | | The user privilege level *level* command already executed | Determined by the *level* argument |

## Configuration Example

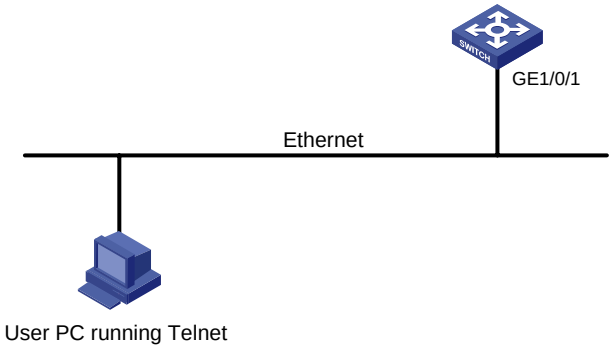
### Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the Console user at the following aspects.

- The user is authenticated against the local password when logging in through the Console port.
- The local password is set to 123456 (in plain text).
- The commands of level 2 are available to users logging in to the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

## Network diagram

**Figure 2-6** Network diagram for AUX user interface configuration (with the authentication mode being **password**)




## Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

# Specify to authenticate the user logging in through the Console port using the local password.

```
[Sysname-ui-aux0] authentication-mode password
```

# Set the local password to **123456** (in plain text).

```
[Sysname-ui-aux0] set authentication password simple 123456
```

# Specify commands of level 2 are available to the user logging in to the AUX user interface.

```
[Sysname-ui-aux0] user privilege level 2
```

# Set the baud rate of the Console port to 19200 bps.

```
[Sysname-ui-aux0] speed 19200
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

# Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, to ensure a successful login, the console user needs to change the corresponding configuration of the terminal emulation program running on the PC, to make the configuration consistent with that on the switch. Refer to Setting Up the Connection to the Console Port for details.

# Console Port Login Configuration with Authentication Mode Being Scheme

## Configuration Procedure

Follow these steps to perform Console port login configuration (with authentication mode being **scheme**):

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Configure the authentication mode</td><td>Enter the default ISP domain view</td><td>domain domain name</td><td rowspan="3">Optional<br>By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.<br>If you specify to apply an existing scheme by providing the radius-scheme-name argument, you need to perform the following configuration as well:<br>• Perform AAA-RADIUS configuration on the switch. (Refer to AAA Configuration in the Security Volume for details.)<br>• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)</td></tr>
<tr><td>Specify the AAA scheme to be applied to the domain</td><td>authentication default { hwtacacs- scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }</td></tr>
<tr><td>Quit to system view</td><td>quit</td></tr>
<tr><td colspan="2">Create a local user (Enter local user view.)</td><td>local-user user-name</td><td>Required<br>local user is admin by default.</td></tr>
<tr><td colspan="2">Set the authentication password for the local user</td><td>password { simple | cipher } password</td><td>Required</td></tr>
<tr><td colspan="2">Specify the service type for AUX users</td><td>service-type terminal</td><td>Required</td></tr>
<tr><td colspan="2">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td colspan="2">Enter AUX user interface view</td><td>user-interface aux 0</td><td>—</td></tr>
<tr><td colspan="2">Configure to authenticate users locally or remotely</td><td>authentication-mode scheme [ command-authorization ]</td><td>Required<br>The specified AAA scheme determines whether to authenticate users locally or remotely.<br>Users are authenticated locally by default.</td></tr>
</table>

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure the Console port | Set the baud rate | **speed** speed-value | Optional<br>The default baud rate of the AUX port (also the Console port) is 19,200 bps. |
| | Set the check mode | **parity** { **even** \| **mark** \| **none** \| **odd** \| **space** } | Optional<br>By default, the check mode of a Console port is set to **none**, that is, no check bit. |
| | Set the stop bits | **stopbits** { **1** \| **1.5** \| **2** } | Optional<br>The default stop bits of a Console port is 1. |
| | Set the data bits | **databits** { **5** \| **6** \| **7** \| **8** } | Optional<br>The default data bits of a Console port is 8. |
| Configure the command level available to users logging in to the user interface | | **user privilege level** *level* | Optional<br>By default, commands of level 3 are available to users logging in to the AUX user interface. |
| Define a shortcut key for starting terminal sessions | | **activation-key** *character* | Optional<br>By default, pressing Enter key starts the terminal session. |
| Define a shortcut key for aborting tasks | | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available to the user interface | | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set history command buffer size | | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
| Set the timeout time for the user interface | | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that the level the commands of which are available to users logging in to a switch depends on the **authentication-mode scheme** [ **command-authorization** ] command, and the **user privilege level** *level* command.

## Configuration Example

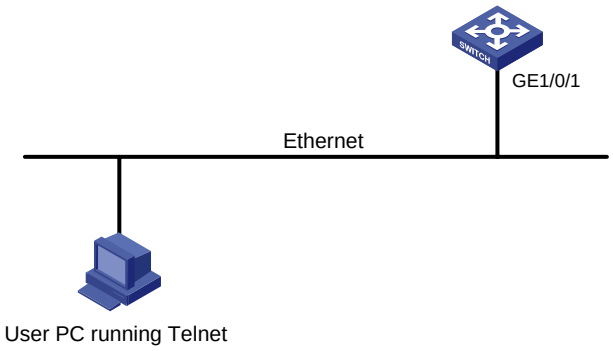
### Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the console user at the following aspects.

- Configure the name of the local user to be “guest”.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of the local user to Terminal.
- Configure to authenticate the user logging in through the Console port in the scheme mode.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

### Network diagram

**Figure 2-7** Network diagram for AUX user interface configuration (with the authentication mode being **scheme**)




### Configuration procedure

# Enter system view.

```
<Sysname> system-view
```

# Create a local user named guest and enter local user view.

```
[Sysname] local-user guest
```

# Set the authentication password to **123456** (in plain text).

```
[Sysname-luser-guest] password simple 123456
```

# Set the service type to Terminal.

```
[Sysname-luser-guest] service-type terminal
[Sysname-luser-guest] quit
```

# Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

# Configure to authenticate the user logging in through the Console port in the scheme mode.

```
[Sysname-ui-aux0] authentication-mode scheme
```

# Set the baud rate of the Console port to 19200 bps.

```
[Sysname-ui-aux0] speed 19200
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

# Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, to ensure a successful login, the console user needs to change the corresponding configuration of the terminal emulation program running on the PC, to make the configuration consistent with that on the switch. Refer to Setting Up the Connection to the Console Port for details.

# 3 Logging In Through Telnet

When logging in through Telnet, go to these sections for information you are interested in:



## Introduction

You can telnet to a remote switch to manage and maintain the switch. To achieve this, you need to configure both the switch and the Telnet terminal properly.

**Table 3-1** Requirements for Telnet to a switch

| Item | Requirement |
|---|---|
| Switch | Start the Telnet Server |
| | The IP address of the VLAN of the switch is configured and the route between the switch and the Telnet terminal is available. |
| | The authentication mode and other settings are configured. Refer to Table 3-2 and Table 3-3. |
| Telnet terminal | Telnet is running. |
| | The IP address of the management VLAN of the switch is available. |

**Note**

- After you log in to the switch through Telnet, you can issue commands to the switch by way of pasting session text, which cannot exceed 2000 bytes, and the pasted commands must be in the same view; otherwise, the switch may not execute the commands correctly.
- If the session text exceeds 2000 bytes, you can save it in a configuration file, upload the configuration file to the switch and reboot the switch with this configuration file. For details, refer to *File System Management* in the *System Volume*.
- To log in on the switch using Telnet based on IPv6 is same as that based on IPv4, and you can refer to *IPv6 Configuration* for details.

## Common Configuration

Table 3-2 lists the common Telnet configuration.

**Table 3-2** Common Telnet configuration

| Configuration | | Remarks |
|---|---|---|
| VTY user interface configuration | Configure the command level available to users logging in to the VTY user interface | Optional<br>By default, commands of level 0 are available to users logging in to a VTY user interface. |
| | Configure the protocols the user interface supports | Optional<br>By default, Telnet and SSH protocol are supported. |
| | Set the command that is automatically executed when a user logs into the user interface | Optional<br>By default, no command is automatically executed when a user logs into a user interface. |
| VTY terminal configuration | Define a shortcut key for aborting tasks | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| | Make terminal services available | Optional<br>By default, terminal services are available in all user interfaces |
| | Set the maximum number of lines the screen can contain | Optional<br>By default, the screen can contain up to 24 lines. |
| | Set history command buffer size | Optional<br>By default, the history command buffer can contain up to 10 commands. |
| | Set the timeout time of a user interface | Optional<br>The default timeout time is 10 minutes. |

**Caution**

- The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.
- Before executing the **auto-execute command** command and save your configuration, make sure you can log in to the switch in other modes and cancel the configuration.

## Telnet Configurations for Different Authentication Modes

Table 3-3 lists Telnet configurations for different authentication modes.

**Table 3-3** Telnet configurations for different authentication modes

| Authentication mode | Telnet configuration | | Remarks |
|---|---|---|---|
| None | Perform common configuration | Perform common Telnet configuration | Optional<br>Refer to Table 3-2. |

| Authentication mode | Telnet configuration | | Remarks |
|---|---|---|---|
| Password | Configure the password | Configure the password for local authentication | Required |
| | Perform common configuration | Perform common Telnet configuration | Optional<br>Refer to Table 3-2. |
| Scheme | Specify to perform local authentication or RADIUS authentication | AAA configuration specifies whether to perform local authentication or RADIUS authentication | Optional<br>Local authentication is performed by default.<br>Refer to AAA Configuration in the Security Volume for details. |
| | Configure user name and password | Configure user names and passwords for local/remote users | Required<br>• The user name and password of a local user are configured on the switch.<br>• The user name and password of a remote user are configured on the RADIUS server. Refer to user manual of RADIUS server for details. |
| | Manage VTY users | Set service type for VTY users | Required |
| | Perform common configuration | Perform common Telnet configuration | Optional<br>Refer to Table 3-2. |

# Telnet Configuration with Authentication Mode Being None

## Configuration Procedure

Follow these steps to perform Telnet configuration (with authentication mode being **none**):

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter one or more VTY user interface views | **user-interface vty** *first-number* [ *last-number* ] | — |
| Configure not to authenticate users logging in to VTY user interfaces | **authentication-mode none** | Required<br>By default, VTY users are authenticated after logging in. |
| Configure the command level available to users logging in to VTY user interface | **user privilege level** *level* | Optional<br>By default, commands of level 0 are available to users logging in to VTY user interfaces. |
| Configure the protocols to be supported by the VTY user interface | **protocol inbound** { **all** \| **ssh** \| **telnet** } | Optional<br>By default, both Telnet protocol and SSH protocol are supported. |

| To do… | Use the command… | Remarks |
| --- | --- | --- |
| Set the command that is automatically executed when a user logs into the user interface | **auto-execute command** *text* | Optional<br>By default, no command is automatically executed when a user logs into a user interface. |
| Define a shortcut key for aborting tasks | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set the history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
| Set the timeout time of the VTY user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that if you configure not to authenticate the users, the command level available to users logging in to a switch depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in Table 3-4.

**Table 3-4** Determine the command level when users logging in to switches are not authenticated

| Scenario | | | Command level |
|---|---|---|---|
| **Authentication mode** | **User type** | **Command** | |
| None (authentication-mode none) | VTY users | The user privilege level *level* command not executed | Level 0 |
| | | The user privilege level *level* command already executed | Determined by the *level* argument |

## Configuration Example

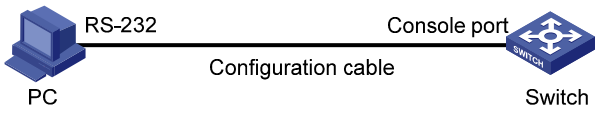
### Network requirements

Assume that you are a level 3 AUX user and want to perform the following configuration for Telnet users logging in to VTY 0:

- Do not authenticate users logging in to VTY 0.
- Commands of level 2 are available to users logging in to VTY 0.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

### Network diagram

**Figure 3-1** Network diagram for Telnet configuration (with the authentication mode being **none**)




### Configuration procedure

# Enter system view, and enable the Telnet service.

```
<Sysname> system-view
[Sysname] telnet server enable
```

# Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

# Configure not to authenticate Telnet users logging in to VTY 0.

```
[Sysname-ui-vty0] authentication-mode none
```

# Specify commands of level 2 are available to users logging in to VTY 0.

```
[Sysname-ui-vty0] user privilege level 2
```

# Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

# Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

## Telnet Configuration with Authentication Mode Being Password

### Configuration Procedure

Follow these steps to perform Telnet configuration (with authentication mode being **password**):

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter one or more VTY user interface views | **user-interface vty** *first-number* [ *last-number* ] | — |
| Configure to authenticate users logging in to VTY user interfaces using the local password | **authentication-mode password** | Required |
| Set the local password | **set authentication password** { **cipher** \| **simple** } *password* | Required |
| Configure the command level available to users logging in to the user interface | **user privilege level** *level* | Optional<br>By default, commands of level 0 are available to users logging in to VTY user interface. |
| Configure the protocol to be supported by the user interface | **protocol inbound** { **all** \| **ssh** \| **telnet** } | Optional<br>By default, both Telnet protocol and SSH protocol are supported. |
| Set the command that is automatically executed when a user logs into the user interface | **auto-execute command** *text* | Optional<br>By default, no command is automatically executed when a user logs into a user interface. |
| Define a shortcut key for aborting tasks | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
| Set the timeout time of the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that if you configure to authenticate the users in the password mode, the command level available to users logging in to a switch depends on both the **authentication-mode password** command and the **user privilege level** *level* command, as listed in Table 3-5.

**Table 3-5** Determine the command level when users logging in to switches are authenticated in the password mode

| Scenario | | | Command level |
|---|---|---|---|
| **Authentication mode** | **User type** | **Command** | |
| Password (authentication-mode password) | VTY users | The user privilege level *level* command not executed | Level 0 |
| | | The user privilege level *level* command already executed | Determined by the *level* argument |

## Configuration Example

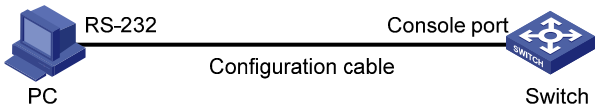
### Network requirements

Assume that you are a level 3 AUX user and want to perform the following configuration for Telnet users logging in to VTY 0:

- Authenticate users logging in to VTY 0 using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to users logging in to VTY 0.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

## Network diagram

**Figure 3-2** Network diagram for Telnet configuration (with the authentication mode being **password**)




## Configuration procedure

# Enter system view, and enable the Telnet service.

```
<Sysname> system-view
[Sysname] telnet server enable
```

# Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

# Configure to authenticate users logging in to VTY 0 using the local password.

```
[Sysname-ui-vty0] authentication-mode password
```

# Set the local password to 123456 (in plain text).

```
[Sysname-ui-vty0] set authentication password simple 123456
```

# Specify commands of level 2 are available to users logging in to VTY 0.

```
[Sysname-ui-vty0] user privilege level 2
```

# Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

# Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

# Telnet Configuration with Authentication Mode Being Scheme

## Configuration Procedure

Follow these steps to perform Telnet configuration (with authentication mode being **scheme**):

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Configure the authenticati on scheme | Enter the default ISP domain view | **domain** *domain name* | Optional<br>By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.<br>If you specify to apply an existing scheme by providing the *radius-scheme-name* argument, you need to perform the following configuration as well:<br>• Perform AAA-RADIUS configuration on the switch. (Refer to AAA Configuration in the Security Volume for details.)<br>• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.) |
| | Configure the AAA scheme to be applied to the domain | **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme- name* [ **local** ] \| **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] } | |
| | Quit to system view | **quit** | |
| Create a local user and enter local user view | | **local-user** *user-name* | No local user exists by default. |
| Set the authentication password for the local user | | **password** { **simple** \| **cipher** } *password* | Required |
| Specify the service type for VTY users | | **service-type telnet** | Required |
| Quit to system view | | **quit** | — |
| Enter one or more VTY user interface views | | **user-interface vty** *first-number* [ *last-number* ] | — |
| Configure to authenticate users locally or remotely | | **authentication-mode scheme** | Required<br>The specified AAA scheme determines whether to authenticate users locally or remotely.<br>Users are authenticated locally by default. |
| Configure the command level available to users logging in to the user interface | | **user privilege level** *level* | Optional<br>By default, commands of level 0 are available to users logging in to the VTY user interfaces. |
| Configure the supported protocol | | **protocol inbound** { **all** \| **ssh** \| **telnet** } | Optional<br>Both Telnet protocol and SSH protocol are supported by default. |
| Set the command that is automatically executed when a user logs into the user interface | | **auto-execute command** *text* | Optional<br>By default, no command is automatically executed when a user logs into a user interface. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Define a shortcut key for aborting tasks | **escape-key** { **default** \| *character* } | Optional<br>The default shortcut key combination for aborting tasks is < Ctrl + C >. |
| Make terminal services available | **shell** | Optional<br>Terminal services are available in all use interfaces by default. |
| Set the maximum number of lines the screen can contain | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
| Set the timeout time for the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging in to a switch depends on the **authentication-mode scheme** [ **command-authorization** ] command and the **user privilege level** *level* command.

**Note**

Refer to *AAA Configuration* and *SSH2.0 Configuration* in the *Security Volume* for configuration about AAA, RADIUS and SSH..

## Configuration Example

### Network requirements

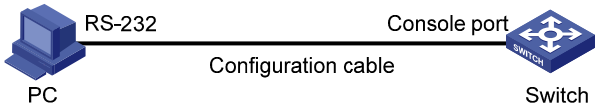
Assume that you are a level 3 AUX user and want to perform the following configuration for Telnet users logging in to VTY 0:

- Configure the name of the local user to be “guest”.
- Set the authentication password of the local user to 123456 (in plain text).

- Set the service type of VTY users to Telnet.
- Configure to authenticate users logging in to VTY 0 in scheme mode.
- The commands of level 2 are available to users logging in to VTY 0.
- Telnet protocol is supported in VTY 0.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

## Network diagram

**Figure 3-3** Network diagram for Telnet configuration (with the authentication mode being **scheme**)




## Configuration procedure

# Enter system view, and enable the Telnet service.

```
<Sysname> system-view
[Sysname] telnet server enable
```

# Create a local user named **guest** and enter local user view.

```
[Sysname] local-user guest
```

# Set the authentication password of the local user to **123456** (in plain text).

```
[Sysname-luser-guest] password simple 123456
```

# Set the service type to Telnet.

```
[Sysname-luser-guest] service-type
```

# Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

# Configure to authenticate users logging in to VTY 0 in the scheme mode.

```
[Sysname-ui-vty0] authentication-mode scheme
```

# Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

# Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

# Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

# Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

# Telnet Connection Establishment

## Telnetting to a Switch from a Terminal

You can telnet to a switch and then configure the switch if the interface of the management VLAN of the switch is assigned with an IP address. (By default, VLAN 1 is the management VLAN.)

Following are procedures to establish a Telnet connection to a switch:

Step 1: Log in to the switch through the Console port, enable the Telnet server function and assign an IP address to the management VLAN interface of the switch.

- Connect to the Console port. Refer to Setting Up the Connection to the Console Port.
- Execute the following commands in the terminal window to enable the Telnet server function and assign an IP address to the management VLAN interface of the switch.

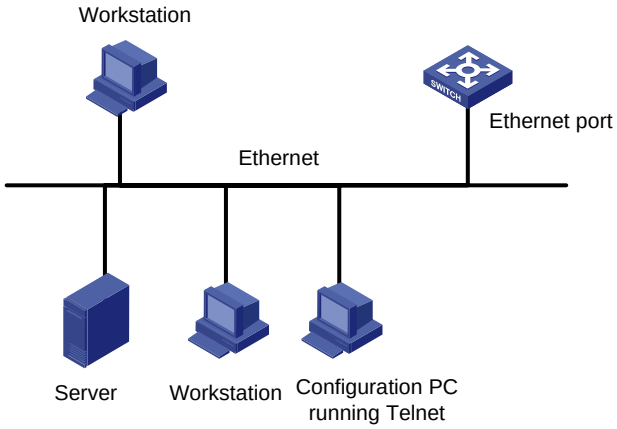
# Enable the Telnet server function and configure the IP address of the management VLAN interface as 202.38.160.92, and .the subnet mask as 255.255.255.0.

```
<Sysname> system-view
[Sysname] telnet server enable
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

Step 2: Before Telnet users can log in to the switch, corresponding configurations should have been performed on the switch according to different authentication modes for them. Refer to Telnet Configuration with Authentication Mode Being None, Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication Mode Being Scheme for details. By default, Telnet users need to pass the password authentication to login.

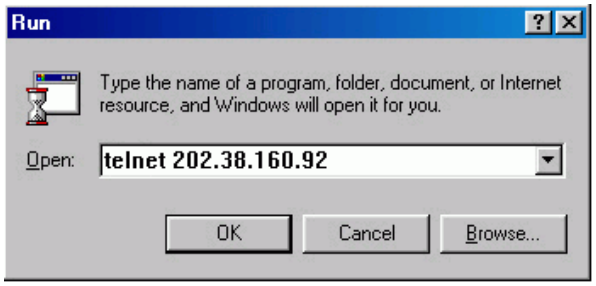
Step 3: Connect your PC to the Switch, as shown in Figure 3-4. Make sure the Ethernet port to which your PC is connected belongs to the management VLAN of the switch and the route between your PC and the switch is available.

**Figure 3-4** Network diagram for Telnet connection establishment




Step 4: Launch Telnet on your PC, with the IP address of the management VLAN interface of the switch as the parameter, as shown in the following figure.

**Figure 3-5** Launch Telnet




Step 5: Enter the password when the Telnet window displays “Login authentication” and prompts for login password. The CLI prompt (such as <4500G>) appears if the password is correct. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”. A 3Com Switch 4500G can accommodate up to five Telnet connections at same time.

Step 6: After successfully Telnetting to a switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the following chapters for the information about the commands.

---

**Note**

- A Telnet connection will be terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.
- By default, commands of level 0 are available to Telnet users authenticated by password. Refer to *Basic System Configuration* in the *System Volume* for information about command hierarchy.

---

## Telnetting to Another Switch from the Current Switch

You can Telnet to another switch from the current switch. In this case, the current switch operates as the client, and the other operates as the server. If the interconnected Ethernet ports of the two switches are in the same LAN segment, make sure the IP addresses of the two management VLAN interfaces to which the two Ethernet ports belong to are of the same network segment, or the route between the two VLAN interfaces is available.

As shown in Figure 3-6, after Telnetting to a switch (labeled as Telnet client), you can Telnet to another switch (labeled as Telnet server) by executing the **telnet** command and then to configure the later.

**Figure 3-6** Network diagram for Telnetting to another switch from the current switch


Step 1: Configure the user name and password for Telnet on the switch operating as the Telnet server. Refer to section Telnet Configuration with Authentication Mode Being None”, section Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication

Mode Being Scheme for details. By default, Telnet users need to pass the password authentication to login.

Step 2: Telnet to the switch operating as the Telnet client.

Step 3: Execute the following command on the switch operating as the Telnet client:

<Sysname> telnet xxxx

Where **xxxx** is the IP address or the host name of the switch operating as the Telnet server. You can use the **ip host** to assign a host name to a switch.

Step 4: Enter the password. If the password is correct, the CLI prompt (such as <4500G>) appears. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”.

Step 5: After successfully Telnetting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the following chapters for the information about the commands.

# 4 Logging in Through Web-based Network Management System

## Introduction

An 3Com Switch 4500G has a Web server built in. You can log in to an 3Com Switch 4500G through a Web browser and manage and maintain the switch intuitively by interacting with the built-in Web server.

To log in to an 3Com Switch 4500G through the built-in Web-based network management system, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

**Table 4-1** Requirements for logging in to a switch through the Web-based network management system

| Item | Requirement |
|---|---|
| Switch | Start the Web server |
| | The IP address of the management VLAN of the switch is configured. The route between the switch and the network management terminal is available. (Refer to the module “IP Addressing and Performance” and “IP Routing” for more.) |
| | The user name and password for logging in to the Web-based network management system are configured. |
| PC operating as the network management terminal | IE is available. |
| | The IP address of the management VLAN interface of the switch is available. |

## HTTP Connection Establishment

Step 1: Log in to the switch through the console port and assign an IP address to the management VLAN interface of the switch. By default, VLAN 1 is the management VLAN.

- Connect to the console port. Refer to section Setting Up the Connection to the Console Port.
- Execute the following commands in the terminal window to assign an IP address to the management VLAN interface of the switch.

# Configure the IP address of the management VLAN interface to be 10.153.17.82 with the mask 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 10.153.17.82 255.255.255.0
```

Step 2: Configure the user name and the password for the Web-based network management system.

# Configure the user name to be admin.

```
[Sysname] local-user admin
```

# Set the password to admin.

```
[Sysname-luser-admin] password simple admin
```

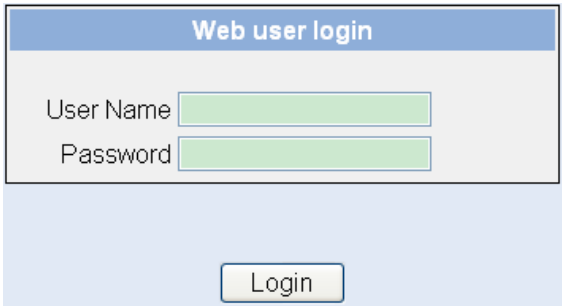
Step 3: Establish an HTTP connection between your PC and the switch, as shown in the following figure.

**Figure 4-1** Establish an HTTP connection between your PC and the switch


Step 4: Log in to the switch through IE. Launch IE on the Web-based network management terminal (your PC) and enter the IP address of the management VLAN interface of the switch (here it is http://10.153.17.82). (Make sure the route between the Web-based network management terminal and the switch is available.)

Step 5: When the login interface (shown in Figure 4-2) appears, enter the user name and the password configured in step 2 and click <Login> to bring up the main page of the Web-based network management system.

**Figure 4-2** The login page of the Web-based network management system




## Web Server Shutdown/Startup

You can shut down or start up the Web server.

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Shut down the Web server | **undo ip http enable** | Required<br>Execute this command in system view.<br>The Web server is started by default. |
| Start the Web server | **ip http enable** | Required<br>Execute this command in system view. |

## Displaying Web Users

After the above configurations, execute the **display** command in any view to display the information about Web users, and thus to verify the configuration effect.

**Table 4-2** Display information about Web users

| To do… | Use the command… |
| --- | --- |
| Display information about Web users | **display web users** |

# 5 Logging In Through NMS

When logging in through NMS, go to these sections for information you are interested in:



## Introduction

You can also log in to a switch through an NMS (network management station), and then configure and manage the switch through the agent module on the switch.

- The agent here refers to the software running on network devices (switches) and as the server.
- SNMP (simple network management protocol) is applied between the NMS and the agent.

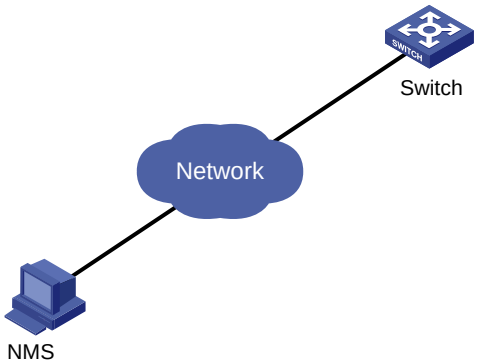
To log in to a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

**Table 5-1** Requirements for logging in to a switch through an NMS

| Item | Requirement |
|---|---|
| Switch | The IP address of the management VLAN of the switch is configured. The route between the NMS and the switch is available. |
| | The basic SNMP functions are configured. (Refer to *SNMP Configuration* in the *System Volume* for details.) |
| NMS | The NMS is properly configured. (Refer to the user manual of the NMS for details.) |

## Connection Establishment Using NMS

**Figure 5-1** Network diagram for logging in through an NMS



# 6 Specifying Source for Telnet Packets

When specifying source IP address/interface for Telnet packets, go to these sections for information you are interested in:



## Introduction

To improve security and make it easier to manage services, you can specify source IP addresses/interfaces for Telnet clients.

Usually, VLAN interface IP addresses and Loopback interface IP addresses are used as the source IP addresses of Telnet packets. After you specify the IP address of a VLAN interface or a Loopback interface as the source IP address of Telnet packets, all the packets exchanged between the Telnet client and the Telnet server use the IP address as their source IP addresses, regardless of the ports through which they are transmitted. In such a way, the actual IP addresses used are concealed. This helps to improve security. Specifying source IP address/interfaces for Telnet packets also provides a way to successfully connect to servers that only accept packets with specific source IP addresses.

## Specifying Source IP address/Interface for Telnet Packets

The configuration can be performed in user view and system view. The configuration performed in user view only applies to the current session. Whereas the configuration performed in system view applies to all the subsequent sessions. Priority in user view is higher than that in system view.

### Specifying source IP address/interface for Telnet packets in user view

Follow these steps to specify source IP address/interface for Telnet packets in user view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify source IP address/interface for Telnet packets (the switch operates as a Telnet client) | **telnet** *remote-system* [ *port-number* ] [ **source** { **ip** *ip-address* \| **interface** *interface-type interface-number* } ] | Optional<br>By default, no source IP address/interface is specified. |

### Specifying source IP address/interface for Telnet packets in system view

Follow these steps to specify source IP address/interface for Telnet packets in system view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify source IP address/interface for Telnet packets | **telnet client source** { **ip** *ip-address* \| **interface** *interface-type interface-number* } | Optional<br>By default, no source IP address/interface is specified. |

**Note**

- The IP address specified must be a local IP address.
- When specifying the source interface for Telnet packets, make sure the interface already exists.
- Before specifying the source IP address/interface for Telnet packets, make sure the route between the interface and the Telnet server is reachable.

## Displaying the source IP address/Interface Specified for Telnet Packets

Follow these steps to display the source IP address/interface specified for Telnet packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the source IP address/interface specified for Telnet packets | **display telnet client configuration** | Available in any view |

# 7 Controlling Login Users

When controlling login users, go to these sections for information you are interested in:



## Introduction

Multiple ways are available for controlling different types of login users, as listed in Table 7-1.

**Table 7-1** Ways to control different types of login users

| Login mode | Control method | Implementation | Related section |
|---|---|---|---|
| Telnet | By source IP addresses | Through basic ACLs | Controlling Telnet Users by Source IP Addresses |
| | By source and destination IP addresses | Through advanced ACLs | Controlling Telnet Users by Source and Destination IP Addresses |
| | By source MAC addresses | Through Layer 2 ACLs | Controlling Telnet Users by Source MAC Addresses |
| SNMP | By source IP addresses | Through basic ACLs | Controlling Network Management Users by Source IP Addresses |

## Controlling Telnet Users

### Prerequisites

The controlling policy against Telnet users is determined, including the source and destination IP addresses to be controlled and the controlling actions (permitting or denying).

### Controlling Telnet Users by Source IP Addresses

This configuration needs to be implemented by basic ACL; a basic ACL ranges from 2000 to 2999. For the definition of ACL, refer to *ACL Configuration* in the *Security Volume*.

Follow these steps to control Telnet users by source IP addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic ACL or enter basic ACL view | **acl** [ **ipv6** ] **number** *acl-number* [ **match-order** { **config** \| **auto** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **permit** \| **deny** } [ **source** { *sour-addr sour-wildcard* \| **any** } \| **time-range** *time-name* \| **fragment** \| **logging** ]* | Required |
| Quit to system view | **quit** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Apply the ACL to control Telnet users by source IP addresses | **acl** [ **ipv6** ] *acl-number* { **inbound** \| **outbound** } | Required<br>The **inbound** keyword specifies to filter the users trying to Telnet to the current switch.<br>The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch. |

## Controlling Telnet Users by Source and Destination IP Addresses

This configuration needs to be implemented by advanced ACL; an advanced ACL ranges from 3000 to 3999. For the definition of ACL, refer to *ACL Configuration* in the *Security Volume*.

Follow these steps to control Telnet users by source and destination IP addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an advanced ACL or enter advanced ACL view | **acl** [ **ipv6** ] **number** *acl-number* [ **match-order** { **config** \| **auto** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **permit** \| **deny** } *rule-string* | Required<br>You can define rules as needed to filter by specific source and destination IP addresses. |
| Quit to system view | **quit** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Apply the ACL to control Telnet users by specified source and destination IP addresses | **acl** [ **ipv6** ] *acl-number* { **inbound** \| **outbound** } | Required<br>The **inbound** keyword specifies to filter the users trying to Telnet to the current switch.<br>The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch. |

## Controlling Telnet Users by Source MAC Addresses

This configuration needs to be implemented by Layer 2 ACL; a Layer 2 ACL ranges from 4000 to 4999. For the definition of ACL, refer to *ACL Configuration* in the *Security Volume*.

Follow these steps to control Telnet users by source MAC addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic ACL or enter basic ACL view | **acl number** *acl-number* [ **match-order** { **config** \| **auto** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **permit** \| **deny** } *rule-string* | Required<br>You can define rules as needed to filter by specific source MAC addresses. |
| Quit to system view | **quit** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Apply the ACL to control Telnet users by source MAC addresses | **acl** *acl-number* **inbound** | Required<br>The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. |

**Note**

Layer 2 ACL is invalid for this function if the source IP address of the Telnet client and the interface IP address of the Telnet server are not in the same subnet.

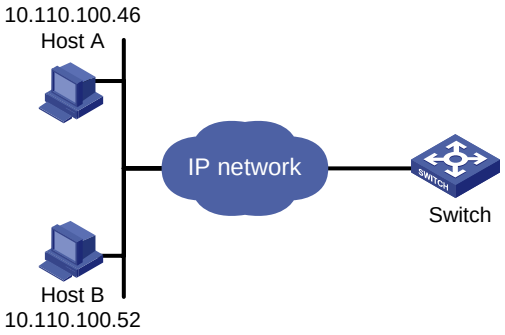
## Configuration Example

### Network requirements

Only the Telnet users sourced from the IP address of 10.110.100.52 and 10.110.100.46 are permitted to log in to the switch.

### Network diagram

**Figure 7-1** Network diagram for controlling Telnet users using ACLs




### Configuration procedure

# Define a basic ACL.

```
<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

# Apply the ACL.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

## Controlling Network Management Users by Source IP Addresses

You can manage an 3Com Switch 4500G through network management software. Network management users can access switches through SNMP.

You need to perform the following two operations to control network management users by source IP addresses.

- Defining an ACL
- Applying the ACL to control users accessing the switch through SNMP

### Prerequisites

The controlling policy against network management users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

## Controlling Network Management Users by Source IP Addresses

Follow these steps to control network management users by source IP addresses:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic ACL or enter basic ACL view | **acl number** *acl-number* [ **match-order** { **config** \| **auto** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **permit** \| **deny** } [ **source** { *sour-addr sour-wildcard* \| **any** } \| **time-range** *time-name* \| **fragment** \| **logging** ]* | Required |
| Quit to system view | **quit** | — |
| Apply the ACL while configuring the SNMP community name | **snmp-agent community** { **read** \| **write** } *community-name* [ **mib-view** *view-name* \| **acl** *acl-number* ]* | Required<br>According to the SNMP version and configuration customs of NMS users, you can reference an ACL when configuring community name, group name or username. For the detailed configuration, refer to *SNMP Configuration* in the *System Volume*. |
| Apply the ACL while configuring the SNMP group name | **snmp-agent group** { **v1** \| **v2c** } *group-name* [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ]<br>**snmp-agent group v3** *group-name* [ **authentication** \| **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | |
| Apply the ACL while configuring the SNMP user name | **snmp-agent usm-user** { **v1** \| **v2c** } *user-name group-name* [ **acl** *acl-number* ]<br>**snmp-agent usm-user v3** *user-name group-name* [ [ **cipher** ] **authentication-mode** { **md5** \| **sha** } *auth-password* [ **privacy-mode** { **aes128** \| **des56** } *priv-password* ] ] [ **acl** *acl-number* ] | |

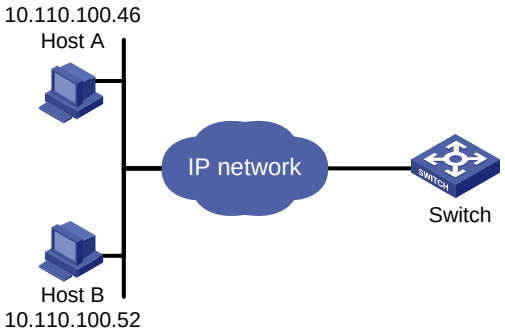
## Configuration Example

### Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 are permitted to access the switch.

## Network diagram

**Figure 7-2** Network diagram for controlling SNMP users using ACLs




## Configuration procedure

# Define a basic ACL.

```
<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

# Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 to access the switch.

```
[Sysname] snmp-agent community read 3com acl 2000
[Sysname] snmp-agent group v2c 3comgroup acl 2000
[Sysname] snmp-agent usm-user v2c 3comuser 3comgroup acl 2000
```

# Table of Contents

# 1 Basic Configurations

While performing basic configurations of the system, go to these sections for information you are interested in:

- Configuration Display
- Basic Configurations
- CLI Features

## Configuration Display

To avoid duplicate configuration, you can use the **display** commands to view the current configuration of the device before configuring the device. The configurations of a device fall into the following categories:

- Factory defaults: When devices are shipped, they are installed with some basic configurations, which are called factory defaults. These default configurations ensure that a device can start up and run normally when it has no configuration file or the configuration file is damaged.
- Current configuration: The currently running configuration on the device.
- Saved configuration: Configurations saved in the startup configuration file.

Follow these steps to display device configurations:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the factory defaults of the device | **display default-configuration** | Available in any view. |
| Display the current validated configurations of the device | **display current-configuration** [ [ **configuration** [ *configuration* ] \| **interface** [ *interface-type* ] [ *interface-number* ] ] [ **by-linenum** ] [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] ] | |
| Display the configuration saved on the storage media of the device | **display saved-configuration** [ **by-linenum** ] | |

**Note**

For details of the **display saved-configuration** command, refer to *File System Management Commands* in the *System Volume.*

## Basic Configurations

This section covers the following topics:

- Entering/Exiting System View

## Entering/Exiting System View

Follow these steps to enter/exit system view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view from user view | **system-view** | — |
| Return to user view from system view | **quit** | — |

**Note**

With the **quit** command, you can return to the previous view. You can execute the **return** command or press the hot key **Ctrl+Z** to return to user view.

## Configuring the Device Name

The device name is used to identify a device in a network. Inside the system, the device name corresponds to the prompt of the CLI. For example, if the device name is **Sysname**, the prompt of user view is <Sysname>.

Follow these steps to configure the device name:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the device name | **sysname** *sysname* | Optional<br>The device name is “4500G” by default. |

## Configuring the System Clock

### Configuring the system clock

The system clock, displayed by system time stamp, is decided by the configured relative time, time zone, and daylight saving time. You can view the system clock by using the **display clock** command.

Follow these steps to configure the system clock:

| To do… | Use the command… | Remarks |
|---|---|---|
| Set time and date | **clock datetime** *time date* | Optional<br>Available in user view. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the time zone | **clock timezone** *zone-name* { **add** \| **minus** } *zone-offset* | Optional |
| Set a daylight saving time scheme | **clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date add-time* | Optional<br>Use either command |
| | **clock summer-time** zone-name **repeating** start-time start-date end-time end-date add-time | |

## Displaying the system clock

The system clock is decided by the commands **clock datetime**, **clock timezone** and **clock summer-time**. If these three commands are not configured, the **display clock** command displays the original system clock. If you combine these three commands in different ways, the system clock is displayed in the ways shown in Table 1-1. The meanings of the parameters in the configuration column are as follows:

- 1 indicates date-time has been configured with the **clock datetime**.
- 2 indicates time-zone has been configured with the **clock timezone** command and the offset time is *zone-offset.*
- 3 indicates daylight saving time has been configured with the **clock summer-time** command and the offset time is *summer-offset.*
- [1] indicates the **clock datetime** command is an optional configuration.
- The default system clock is 2005/1/1 1:00:00 in the example.

**Table 1-1** Relationship between the configuration and display of the system clock

| Configuration | System clock displayed by the display clock command | Example |
|---|---|---|
| 1 | *date-time* | Configure: clock datetime 1:00 2007/1/1<br>Display: 01:00:00 UTC Mon 01/01/2007 |
| 2 | The original system clock ± *zone-offset* | Configure: clock timezone zone-time add 1<br>Display: 02:00:00 zone-time Sat 01/01/2005 |
| 1 and 2 | *date-time* ± *zone-offset* | Configure: clock datetime 2:00 2007/2/2 and clock timezone zone-time add 1<br>Display: 03:00:00 zone-time Fri 02/02/2007 |
| [1], 2 and 1 | *date-time* | Configure: clock timezone zone-time add 1 and clock datetime 3:00 2007/3/3<br>Display: 03:00:00 zone-time Sat 03/03/2007 |

| Configuration | System clock displayed by the display clock command | Example |
|---|---|---|
| 3 | If the original system clock is not in the daylight saving time range, the original system clock is displayed. | Configure: clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2<br>Display: 01:00:00 UTC Sat 01/01/2005 |
| | If the original system clock is in the daylight saving time range, the original system clock + *summer-offset* is displayed. | Configure: clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2<br>Display: 03:00:00 ss Sat 01/01/2005 |
| 1 and 3 | If *date-time* is not in the daylight saving time range, *date-time* is displayed. | Configure: clock datetime 1:00 2007/1/1 and clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2<br>Display: 01:00:00 UTC Mon 01/01/2007 |
| | If *date-time* is in the daylight saving time range, "*date-time"* + "*summer-offset"* is displayed. | Configure: clock datetime 8:00 2007/1/1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2<br>Display: 10:00:00 ss Mon 01/01/2007 |
| [1], 3 and 1 | If *date-time* is not in the daylight saving time range, *date-time* is displayed. | Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 1:00 2008/1/1<br>Display: 01:00:00 UTC Tue 01/01/2008 |
| | *date-time* is in the daylight saving time range:<br>If the value of *"date-time" - "summer-offset"* is not in the summer-time range, *"date-time" - "summer-offset"* is displayed;<br>If the value of *"date-time" - "summer-offset"* is in the summer-time range, *date-time* is displayed. | Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 1:30 2007/1/1<br>Display: 23:30:00 UTC Sun 12/31/2006 |
| | | Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 3:00 2007/1/1<br>Display: 03:00:00 ss Mon 01/01/2007 |
| 2 and 3 or 3 and 2 | If the value of the original system clock ± "zone-offset" is not in the summer-time range, the original system clock ± "zone-offset" is displayed. | Configure: clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2<br>Display: 02:00:00 zone-time Sat 01/01/2005 |
| | | Configure: clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2005/1/1 1:00 2005/8/8 2<br>Display: 04:00:00 ss Sat 01/01/2005 |
| | If the value of the original system clock ± "zone-offset" is in the summer-time range, the original system clock ± "zone-offset" + "summer-offset" is displayed. | Configure: clock datetime 1:00 2007/1/1, clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2<br>Display: 02:00:00 zone-time Mon 01/01/2007 |

| Configuration | System clock displayed by the display clock command | Example |
|---|---|---|
| 1, 2 and 3 or 1, 3 and 2 | If the value of "*date-time*"±"*zone-offset*" is not in the summer-time range, "date-time"±"zone-offset" is displayed. | Configure: clock datetime 1:00 2007/1/1, clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2<br>Display: 04:00:00 ss Mon 01/01/2007 |
| | If the value of "*date-time*"±"*zone-offset*" is in the summer-time range, "date-time"±"zone-offset"+"summer-offset" is displayed. | Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 1:00 2007/1/1<br>Display: 01:00:00 zone-time Mon 01/01/2007 |
| [1], 2, 3 and 1 or [1], 3, 2 and 1 | If *date-time* is not in the daylight saving time range, *date-time* is displayed. | Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 1:30 2008/1/1<br>Display: 23:30:00 zone-time Mon 12/31/2007 |
| | *date-time* is in the daylight saving time range:<br>If the value of *"date-time"-"summer-offset"* is not in the summer-time range, *"date-time"-"summer-offset"* is displayed;<br>If the value of *"date-time"-"summer-offset"* is in the summer-time range, *date-time* is displayed. | Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 3:00 2008/1/1<br>Display: 03:00:00 ss Tue 01/01/2008 |

## Enabling/Disabling the Display of Copyright Information

- With the display of copyright information enabled, the copyright information is displayed when a user logs in through Telnet or SSH, or when a user quits user view after logging in to the device through the console port, AUX port, or asynchronous serial interface. The copyright information will not be displayed under other circumstances. The display format of copyright information is as shown below:

```
**************************************************************************
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
**************************************************************************
```

- With the display of copyright information disabled, under no circumstances will the copyright information be displayed.

Follow these steps to enable/disable the display of copyright information:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the display of copyright information | **copyright-info enable** | Optional<br>Enabled by default. |
| Disable the display of copyright information | **undo copyright-info enable** | Required<br>Enabled by default. |

## Configuring a Banner

### Introduction to banners

Banners are prompt information displayed by the system when users are connected to the device, perform login authentication, and start interactive configuration. The administrator can set corresponding banners as needed.

At present, the system supports the following five kinds of welcome information.

- **shell** banner, also called session banner, displayed when a non TTY Modem user enters user view.
- **incoming** banner, also called user interface banner, displayed when a user interface is activated by a Modem user.
- **login** banner, welcome information at login authentications, displayed when password and scheme authentications are configured.
- **motd** (Message of the Day) banner, welcome information displayed before authentication.
- **legal** banner, also called authorization information. The system displays some copyright or authorization information, and then displays the **legal** banner before a user logs in, waiting for the user to confirm whether to continue the authentication or login. If entering Y or pressing the **Enter** key, the user enters the authentication or login process; if entering N, the user quits the authentication or login process. Y and N are case insensitive.

### Configuring a banner

When you configure a banner, the system supports two input modes. One is to input all the banner information right after the command keywords. The start and end characters of the input text must be the same but are not part of the banner information. In this case, the input text, together with the command keywords, cannot exceed 510 characters. The other is to input all the banner information in multiple lines by pressing the **Enter** key. In this case, up to 2000 characters can be input.

The latter input mode can be achieved in the following three ways:

- Press the **Enter** key directly after the command keywords, and end the setting with the % character. The **Enter** and % characters are not part of the banner information.
- Input a character after the command keywords at the first line, and then press the **Enter** key. End the setting with the character input at the first line. The character at the first line and the end character are not part of the banner information.
- Input multiple characters after the command keywords at the first line (with the first and last characters being different), then press the **Enter** key. End the setting with the first character at the first line. The first character at the first line and the end character are not part of the banner information.

Follow these steps to configure a banner:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the banner to be displayed at login (available for Modem login users) | **header incoming** *text* | Optional |
| Configure the banner to be displayed at login authentication | **header login** *text* | Optional |
| Configure the authorization information before login | **header legal** *text* | Optional |
| Configure the banner to be displayed when a user enters user view (non Modem login users) | **header shell** *text* | Optional |
| Configure the banner to be displayed before login | **header motd** *text* | Optional |

## Configuring CLI Hotkeys

Follow these steps to configure CLI hotkeys:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure CLI hotkeys | **hotkey** { **CTRL_G** \| **CTRL_L** \| **CTRL_O** \| **CTRL_T** \| **CTRL_U** } *command* | Optional<br>The **Ctrl+G**, **Ctrl+L** and **Ctrl+O** hotkeys are specified with command lines by default. |
| Display hotkeys | **display hotkey** | Available in any view. Refer to Table 1-2 for hotkeys reserved by the system. |

**Note**

By default, the **Ctrl+G**, **Ctrl+L** and **Ctrl+O** hotkeys are configured with command line and the **Ctrl+T** and **Ctrl+U** commands are NULL.

- **Ctrl+G** corresponds to the **display current-configuration** command.
- **Ctrl+L** corresponds to the **display ip routing-table** command.
- **Ctrl+O** corresponds to the **undo debugging all** command.

**Table 1-2** Hotkeys reserved by the system

| Hotkey | Function |
|---|---|
| **Ctrl+A** | Moves the cursor to the beginning of the current line. |
| **Ctrl+B** | Moves the cursor one character to the left. |
| **Ctrl+C** | Stops performing a command. |
| **Ctrl+D** | Deletes the character at the current cursor position. |
| **Ctrl+E** | Moves the cursor to the end of the current line. |

| Hotkey | Function |
|---|---|
| **Ctrl+F** | Moves the cursor one character to the right. |
| **Ctrl+H** | Deletes the character to the left of the cursor. |
| **Ctrl+K** | Terminates an outgoing connection. |
| **Ctrl+N** | Displays the next command in the history command buffer. |
| **Ctrl+P** | Displays the previous command in the history command buffer. |
| **Ctrl+R** | Redisplays the current line information. |
| **Ctrl+V** | Pastes the content in the clipboard. |
| **Ctrl+W** | Deletes all the characters in a continuous string to the left of the cursor. |
| **Ctrl+X** | Deletes all the characters to the left of the cursor. |
| **Ctrl+Y** | Deletes all the characters to the right of the cursor. |
| **Ctrl+Z** | Exits to user view. |
| **Ctrl+]** | Terminates an incoming connection or a redirect connection. |
| **Esc+B** | Moves the cursor to the leading character of the continuous string to the left. |
| **Esc+D** | Deletes all the characters of the continuous string at the current cursor position and to the right of the cursor. |
| **Esc+F** | Moves the cursor to the front of the next continuous string to the right. |
| **Esc+N** | Moves the cursor down by one line (available before you press **Enter**) |
| **Esc+P** | Moves the cursor up by one line (available before you press **Enter**) |
| **Esc+<** | Specifies the cursor as the beginning of the clipboard. |
| **Esc+>** | Specifies the cursor as the ending of the clipboard. |

**Note**

These hotkeys are defined by the device. When you interact with the device from terminal software, these keys may be defined to perform other operations. If so, the definition of the terminal software will dominate.

## Configuring User Privilege Levels and Command Levels

### Introduction

To restrict the different users' access to the device, the system manages the users by their privilege levels. User privilege levels correspond to command levels. After users at different privilege levels log in, they can only use commands at their own, or lower, levels. All the commands are categorized into four levels, which are visit, monitor, system, and manage from low to high, and identified respectively by 0 through 3. Table 1-3 describes the levels of the commands.

**Table 1-3** Default command levels

| Level | Privilege | Description |
|---|---|---|
| 0 | Visit | Involves commands for network diagnosis and commands for accessing an external device. Commands at this level are not allowed to be saved after being configured. After the device is restarted, the commands at this level will be restored to the default settings. Commands at this level include **ping**, **tracert**, **telnet** and **ssh2**. |
| 1 | Monitor | Includes commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the device is restarted, the commands at this level will be restored to the default settings. Commands at this level include **debugging**, **terminal**, **refresh**, **reset**, and **send**. |
| 2 | System | Provides service configuration commands, including routing and commands at each level of the network for providing services. By default, commands at this level include all configuration commands except for those at manage level. |
| 3 | Manage | Influences the basic operation of the system and the system support modules for service support. By default, commands at this level involve file system, FTP, TFTP, Xmodem command download, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands). |

## Configuring user privilege level

User privilege level can be configured by using AAA authentication parameters or under a user interface.

1) Configure user privilege level by using AAA authentication parameters

If the user interface authentication mode is **scheme** when a user logs in, and username and password are needed at login, then the user privilege level is specified in the configuration of AAA authentication.

Follow these steps to configure user privilege level by using AAA authentication parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Configure the authentication mode for logging in to the user interface as **scheme** | **authentication-mode scheme** [ **command-authorization** ] | Required<br>By default, the authentication mode for VTY and AUX users is **password**. |
| Exit to system view | **quit** | — |
| Configure the authentication mode for SSH users as **password** | For the details, refer to *SSH2.0 Configuration* in the *Security Volume.* | Required if users use SSH to log in, and username and password are needed at authentication |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure the user privilege level by using AAA authentication parameters | Using local authentication | • Use the **local-user** command to create a local user and enter local user view.<br>• Use the **level** keyword in the **authorization-attribute** command to configure the user level. | User either approach<br>• For local authentication, if you do not configure the user level, the user level is 0, that is, users of this level can use commands with level 0 only.<br>• For remote authentication, if you do not configure the user level, the user level depends on the default configuration of the authentication server. |
| | Using remote authentication (RADIUS, HWTACACS, and LDAP authentications) | Configure user level on the authentication server | |

**Note**

- For the description of user interface, refer to *Login Configuration* in the *System Volume*; for the description of the **user-interface**, **authentication-mode** and **user privilege level** commands, refer to *User Interface Commands* in the *System Volume*.
- For the introduction to AAA authentication, refer to *AAA Configuration* in the *Security Volume*; for the description of the **local-user** and **authorization-attribute** commands, refer to *AAA Commands* in the *Security Volume*.
- For the introduction to SSH, refer to *SSH 2.0 Configuration* in the *Security Volume*.

2) Example of configuring user privilege level by using AAA authentication parameters

# Authenticate the users telnetting to the device through VTY 1, verify their usernames and passwords locally, and specify the user privilege level as 3.

```
<Sysname> system-view
[Sysname] user-interface vty 1
[Sysname-ui-vty1] authentication-mode scheme
[Sysname-ui-vty1] quit
[Sysname] local-user test
[Sysname-luser-test] password cipher 123
[Sysname-luser-test] service-type telnet
```

After the above configuration, when users telnet to the device through VTY 1, they need to input username **test** and password **123**. After passing the authentication, users can only use the commands of level 0. If the users need to use commands of levels 0, 1, 2 and 3, the following configuration is required:

```
[Sysname-luser-test] authorization-attribute level 3
```

3) Configure the user privilege level under a user interface

If the user interface authentication mode is **scheme** when a user logs in, and SSH **publickey** authentication type (only username is needed for this authentication type) is adopted, then the user privilege level is the user interface level; if a user logs in using the **none** or **password** mode (namely, no username is needed), the user privilege level is the user interface level.

Follow these steps to configure the user privilege level under a user interface (SSH **publickey** authentication type):

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the authentication type for SSH users as **publickey** | For the details, refer to *SSH2.0 Configuration* in the *Security Volume*. | Required if users adopt the SSH login mode, and only username, instead of password is needed at authentication.<br>After the configuration, the authentication mode of the corresponding user interface must be set to **scheme**. |
| Enter system view | **system-view** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Configure the authentication mode when a user uses the current user interface to log in to the device | **authentication-mode scheme** [ **command-authorization** ] | Optional<br>By default, the authentication mode for VTY and AUX user interfaces is **password**. |
| Configure the privilege level of the user logging in from the current user interface | **user privilege level** *level* | Optional<br>By default, the user privilege level for users logging in from the console user interface is 3, and that for users logging from the other user interfaces is 0. |

Follow these steps to configure the user privilege level under a user interface (**none** or **password** authentication mode):

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |
| Configure the authentication mode when a user uses the current user interface to log in to the device | **authentication-mode** { **none** \| **password** } | Optional<br>By default, the authentication mode for VTY and AUX user interfaces is **password**. |
| Configure the privilege level of the user logging in from the current user interface | **user privilege level** *level* | Optional<br>By default, the user privilege level for users logging in from the console user interface is 3, and that for users logging from the other user interfaces is 0. |

4) Example of configuring user privilege level under a user interface

- Perform no authentication to the users telnetting to the device, and specify the user privilege level as 1. (This configuration brings potential security problem. Therefore, you are recommended to use it only in a lab environment.)

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode none
```

```
[Sysname-ui-vty0-4] user privilege level 1
```

By default, when users telnet to the device, they can only use the following commands after passing the authentication:

```
<Sysname> ?
User view commands:
  cluster        Run cluster command
  display        Display current system information
  ping           Ping function
  quit           Exit from current command view
  ssh2           Establish a secure shell client connection
  super          Set the current user priority level
  telnet         Establish one TELNET connection
  tracert        Trace route function
```

After you set the user privilege level under the user interface, users can log in to the device through Telnet without any authentication and use the following commands:

```
<Sysname> ?
User view commands:
  cluster        Run cluster command
  debugging      Enable system debugging functions
  display        Display current system information
  ipc            Interprocess communication
  ping           Ping function
  quit           Exit from current command view
  refresh        Do soft reset
  reset          Reset operation
  screen-length  Specify the lines displayed on one screen
  send           Send information to other user terminal interface
  ssh2           Establish a secure shell client connection
  super          Set the current user priority level
  telnet         Establish one TELNET connection
  terminal       Set the terminal line characteristics
  tracert        Trace route function
  undo           Cancel current setting
```

- Authenticate the usesr logging in to the device through Telnet, verify their passwords, and specify the user privilege levels as 2.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty1] authentication-mode password
[Sysname-ui-vty0-4] set authentication password cipher 123
[Sysname-ui-vty0-4] user privilege level 2
```

By default, when users log in to the device through Telnet, they can use the commands of level 0 after passing the authentication. After you set the user privilege level under the user interface, when users log in to the device through Telnet, they need to input password **123**, and then they can use commands of levels 0, 1, and 2.

### Switching user privilege level

Users can switch their user privilege level temporarily without logging out and disconnecting the current connection; after the switch, users can continue to configure the device without the need of relogin and reauthentication, but the commands that they can execute have changed. For example, if the current user privilege level is 3, the user can configure system parameters; after switching the user privilege level to 0, the user can only execute some simple commands, like **ping** and **tracert**, and only a few **display** commands. The switching of user privilege level is temporary, and effective for the current login; after the user relogs in, the user privilege restores to the original level.

To avoid misoperations, the administrators are recommended to log in to the device by using a lower privilege level and view device operating parameters, and when they have to maintain the device, they can switch to a higher level temporarily; when the administrators need to leave for a while or ask someone else to manage the device temporarily, they can switch to a lower privilege level before they leave to restrict the operation by others.

Users can switch from a high user privilege level to a low user privilege level without entering a password; when switching from a low user privilege level to a high user privilege level, only the console login users do not have to enter the password, and users that log in from VTY user interfaces need to enter the password for security's sake. This password is for level switching only and is different from the login password. If the entered password is incorrect or no password is configured, the switching fails. Therefore, before switching a user to a higher user privilege level, you should configure the password needed.

Follow these steps to switch user privilege level:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the password for switching the user privilege level | **super password** [ **level** *user-level* ] { **simple** \| **cipher** } *password* | Required<br>By default, no password is configured. |
| Exit to user view | **quit** | — |
| Switch the user privilege level | **super** [ *level* ] | Required<br>When logging in to the device, a user has a user privilege level, which is decided by user interface or authentication user level. |

**Caution**

- When you configure the password for switching user privilege level with the **super password** command, the user privilege level is 3 if no user privilege level is specified.
- The password for switching user privilege level can be displayed in both cipher text and simple text. You are recommended to adopt the former as the latter is easily cracked.

### Modifying command level

All the commands in a view are defaulted to different levels, as shown in Table 1-3. The administrator can modify the command level based on users' needs to make users of a lower level use commands with a higher level or improve device security.

Follow these steps to modify the command level:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the command level in a specified view | **command-privilege level** *level* **view** *view command* | Required<br>Refer to Table 1-3 for the default settings. |

**Caution**

You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.

## Displaying and Maintaining Basic Configurations

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information on system version | **display version** | Available in any view |
| Display information on the system clock | **display clock** | |
| Display information on terminal users | **display users** [ **all** ] | |
| Display the valid configuration under current view | **display this** [ **by-linenum** ] | |
| Display clipboard information | **display clipboard** | |
| Display and save statistics of each module's running status | **display diagnostic-information** | |

During daily maintenance or when the system is operating abnormally, you need to view each module's running status to find the problem. Therefore, you are required to execute the corresponding **display** commands one by one. To collect more information one time, you can execute the **display diagnostic-information** command in any view to display or save statistics of each module's running status. The execution of the **display diagnostic-information** command has the same effect as that of the commands **display clock**, **display version**, **display device**, and **display current-configuration**.

**Note**

- For the detailed description of the display users command, refer to *Login Commands* in the System Volume.
- Support for the display configure-user and display current-configuration command depends on the device model.
- The display commands discussed above are for the global configuration. Refer to the corresponding section for the display command for specific protocol and interface.

# CLI Features

This section covers the following topics:



## Introduction to CLI

CLI is an interaction interface between devices and users. Through CLI, you can configure your devices by entering commands and view the output information and verify your configurations, thus facilitating your configuration and management of your devices.

CLI provides the following features for you to configure and manage your devices:

- Hierarchical command protection where you can only execute the commands at your own or lower levels. Refer to Configuring User Privilege Levels and Command Levels for details.
- Easy access to on-line help by entering “?”
- Abundant debugging information for fault diagnosis
- Saving and executing commands that have been executed
- Fuzzy match for convenience of input. When you execute a command, you can input part of the characters in a keyword. However, to enable you to confirm your operation, the command can be executed only when you input enough characters to make the command unique. Take the commands **save**, **startup saved-configuration**, and **system-view** which start with **s** as an example. To save the current configuration, you need to input **sa** at least; to set the configuration file for next startup, you need to input **st s** at least; to enter system view, you need to input **sy** at least. You can press **Tab** to complement the command, or you can input the complete command.

## Online Help with Command Lines

The following are the types of online help available with the CLI:

- Full help
- Fuzzy help

To obtain the desired help information, you can:

1) Enter **?** in any view to access all the commands in this view and brief description about them as well.

```
<Sysname> ?
User view commands:
  backup              Backup next startup-configuration file to TFTP server
  boot-loader         Set boot loader
  bootrom             Update/read/backup/restore bootrom
  cd                  Change current directory
  clock               Specify the system clock
  cluster             Run cluster command
  copy                Copy from one file to another
  debugging           Enable system debugging functions
  delete              Delete a file
  dir                 List files on a file system
  display             Show running system information
......omitted......
```

2) Enter a command and a **?** separated by a space. If **?** is at the position of a keyword, all the keywords are given with a brief description.

```
<Sysname> terminal ?
  debugging  Send debug information to terminal
  logging    Send log information to terminal
  monitor    Send information output to current terminal
  trapping   Send trap information to terminal
```

3) Enter a command and a **?** separated by a space. If **?** is at the position of a parameter, the description about this parameter is given.

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
  <1-4094>  VLAN interface number
[Sysname] interface vlan-interface 1 ?
  <cr>
[Sysname] interface vlan-interface 1
```

Where, <cr> indicates that there is no parameter at this position. The command is then repeated in the next command line and executed if you press **Enter**.

4) Enter a character string followed by a **?**. All the commands starting with this string are displayed.

```
<Sysname> c?
   cd
   clock
   copy
```

5) Enter a command followed by a character string and a **?.** All the keywords starting with this string are listed.

```
<Sysname> display ver?
   version
```

6) Press **Tab** after entering the first several letters of a keyword to display the complete keyword, provided these letters can uniquely identify the keyword in this command. If several matches are found, the complete keyword which is matched first is displayed (the matching rule is: the letters next to the input letters are arranged in alphabetic order, and the letter in the first place is matched

first.). If you repeatedly press **Tab**, all the keywords starting with the letter that you enter are displayed in cycles.

## Synchronous Information Output

Synchronous information output refers to the feature that if the user's input is interrupted by system output, then after the completion of system output the system will display a command line prompt and your input so far, and you can continue your operations from where you were stopped.

You can use the **info-center synchronous** command to enable synchronous information output. For the detailed description of this function, refer to *Information Center Configuration* in the *System Volume*.

## Undo Form of a Command

Adding the keyword **undo** can form an **undo** command. Almost every configuration command has an **undo** form. **undo** commands are generally used to restore the system default, disable a function or cancel a configuration. For example, the **info-center enable** command is used to enable the information center, while the **undo info-center enable** command is used to disable the information center. (By default, the information center is enabled.)

## Editing Features

The CLI provides the basic command editing functions and supports multi-line editing. When you execute a command, the system automatically goes to the next line if the maximum length of the command is reached. You cannot press **Enter** to go to the next line; otherwise, the system will automatically execute the command. The maximum length of each command is 510 characters. Table 1-4 lists these functions.

**Table 1-4** Edit functions

| Key | Function |
|---|---|
| Common keys | If the editing buffer is not full, insert the character at the position of the cursor and move the cursor to the right. |
| **Backspace** | Deletes the character to the left of the cursor and move the cursor back one character. |
| Left-arrow key or **Ctrl+B** | The cursor moves one character space to the left. |
| Right-arrow key or **Ctrl+F** | The cursor moves one character space to the right. |
| Up-arrow key or **Ctrl+P** | Displays history commands |
| Down-arrow key or **Ctrl+N** | |
| **Tab** | Pressing **Tab** after entering part of a keyword enables the fuzzy help function. If finding a unique match, the system substitutes the complete keyword for the incomplete one and displays it in the next line; when there are several matches, if you repeatedly press **Tab**, all the keywords starting with the letter that you enter are displayed in cycles. If there is no match at all, the system does not modify the incomplete keyword and displays it again in the next line. |

**Note**

When editing the command line, you can use other shortcut keys (For details, see Table 1-2) besides the shortcut keys defined in Table 1-4, or you can define shortcut keys by yourself. (For details, see Configuring CLI Hotkeys.)

## CLI Display

By filtering the output information, you can find the wanted information effectively. If there is a lot of information to be displayed, the system displays the information in multiple screens. When the information is displayed in multiple screens, you can also filter the output information to pick up the wanted information.

### Filtering the output information

The device provides the function to filter the output information. You can specify a regular expression (that is, the output rule) to search information you need.

You can use one of the following two ways to filter the output information:

- Input the keyword **begin**, **exclude**, or **include** as well as the regular expression at the command line to filter the output information.
- Input slash (/), minus (-), or plus (+) as well as the regular expression to filter the rest output information. Slash (/) is equal to the keyword **begin**, minus (-) is equal to the keyword **exclude**, and plus (+) is equal to the keyword **include**.

Keywords **begin**, **exclude**, and **include** have the following meanings:

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays only the lines that match the regular expression.

The regular expression is a string of 1 to 256 characters, case sensitive. It also supports special characters as shown in Table 1-5.

**Table 1-5** Special characters in a regular expression

| Character | Meaning | Remarks |
|---|---|---|
| ^string | Starting sign, string appears only at the beginning of a line. | For example, regular expression “^user” only matches a string beginning with “user”, not “Auser”. |
| string$ | Ending sign, string appears only at the end of a line. | For example, regular expression "user$” only matches a string ending with “user”, not “userA”. |
| . | Full stop, a wildcard used in place of any character, including single character, special character and blank. | For example, “.l” can match “vlan” or “mpls”. |
| * | Asterisk, used to match a character or character group before it zero or multiple times. | For example, “zo*” can match “z” and “zoo”; (zo)* can match “zo” and “zozo”. |

| Character | Meaning | Remarks |
|---|---|---|
| + | Addition, used to match a character or character group one or multiple times before it | For example, “zo+” can match “zo” and “zoo”, but not “z”. |
| \| | Vertical bar, used to match the whole string on the left or right of it | For example, “def\|int” can only match a character string containing “def” or “int”. |
| _ | Underline. If it is at the beginning or the end of a regular expression, it equals ^ or $; in other cases, it equals comma, space, round bracket, or curly bracket. | For example, “a_b” can match “a b” or “a(b”; “_ab” can only match a line starting with “ab”; “ab_” can only match a line ending with “ab”. |
| - | Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ]. | For example, “1-9” means numbers from 1 to 9 (inclusive); “a-h” means from a to h (inclusive). |
| [ ] | A range of characters, Matches any character in the specified range. | For example, [16A] can match a string containing any character among 1, 6, and A; [1-36A] can match a string containing any character among 1, 2, 3, 6, and A (with - being a hyphen).<br>“]” can be matched only when it is put at the beginning of [ ] if it is used as a common character in [ ], for example [ ]*string*]. There is no such limit on “[”. |
| ( ) | A character group. It is usually used with “+” or “*”. | For example, (123A) means a character group “123A”; “408(12)+” can match 40812 or 408121212. But it cannot match 408. |
| *index* | Repeats a specified character group for once. A character group refers to the string in () before \. *index* refers to the sequence number (starting from 1 from left to right) of the character group before \: if only one character group appears before \, then *index* can only be 1; if n character groups appear before *index*, then *index* can be any integer from 1 to n. | For example, (*string*)\1 means to repeat *string* for once, and (*string*)\1 must match a string containing *stringstring;* (*string1*)(*string2*)\2 means to repeat *string2* for once, and (*string1*)(*string2*)\2 must match a string containing *string1string2string2;* (*string1*)(*string2*)\1\2 means to repeat *string1* for once first*,* and then repeat string2 for once*, and* (*string1*)(*string2*)\1\2 must match a string containing *string1string2string1string2.* |
| [^] | Used to match any character not in a specified range. | For example, [^16A] means to match a string containing any character except 1, 6 or A, and the string can also contain 1, 6 or A, but cannot contain these three characters only. For example, [^16A] can match “abc” and “m16”, but not 1, 16, or 16A. |
| \<string | Used to match a character string starting with string. | For example, “\<do” can match word “domain” or string “doa”. |
| string\> | Used to match a character string ending with string. | For example, “do\>” can match word “undo” or string “abcdo”. |

| Character | Meaning | Remarks |
|---|---|---|
| \bcharacter2 | Used to match character1character2. character1 can be any character except number, letter or underline, and \b equals [^A-Za-z0-9_]. | For example, \ba can match -a, with - represents character1, and a represents character2; while \ba cannot match “2a” or “ba”. |
| \Bcharacter | It must match a string containing character, and there can no spaces before character. | For example, “\Bt” can match “t” in “install”, but not “t” in “big top”. |
| character1\w | Used to match character1character2. character2 must be a number, letter or underline, and \w equals [^A-Za-z0-9_]. | For example, “v\w” can match “vlan”, with “v” being character1, and “l” being character2. v\w can also match “service”, with “i” being character2. |
| \W | Equals \b. | For example, “\Wa” can match “-a”, with “-” representing character1, and “a” representing character2; while “\ba” cannot match “2a” or “ba”. |
| \ | Escape character. If single special characters listed in this table follow \, the specific meanings of the characters will be removed. | For example, “\\” can match a string containing “\”, “\^” can match a string containing “^”, and “\\b” can match a string containing “\b”. |

## Multiple-screen output

When there is a lot of information to be output, the system displays the information in multiple screens. Generally, 24 lines are displayed on one screen, and you can also use the **screen-length** command to set the number of lines displayed on the next screen. (For the details of this command, refer to *Login Commands* in the *System Volume*.) You can follow the step below to disable the multiple-screen output function of the current user.

| To do… | Use the command… | Remarks |
|---|---|---|
| Disable the multiple-screen output function of the current user | **screen-length disable** | Required<br>By default, a login user uses the settings of the **screen-length** command. The default settings of the **screen-length** command are: multiple-screen output is enabled and 24 lines are displayed on the next screen.<br>This command is executed in user view, and therefore is applicable to the current user only. When a user re-logs in, the settings restore to the system default. |

## Display functions

CLI offers the following feature:

When the information displayed exceeds one screen, you can pause using one of the methods shown in Table 1-6.

**Table 1-6** Display functions

| Action | Function |
|---|---|
| Press **Space** when information display pauses | Continues to display information of the next screen page. |
| Press **Enter** when information display pauses | Continues to display information of the next line. |
| Press **Ctrl+C** when information display pauses | Stops the display and the command execution. |
| **Ctrl+E** | Moves the cursor to the end of the current line. |
| **PageUp** | Displays information on the previous page. |
| **PageDown** | Displays information on the next page. |

## Saving History Commands

The CLI can automatically save the commands that have been used lately to the history buffer. You can know the operations that have been executed successfully, invoke and repeatedly execute them as needed. By default, the CLI can save up to ten commands for each user. You can use the **history-command max-size** command to set the capacity of the history commands buffer for the current user interface (For the detailed description of the **history-command max-size** command, refer to *Login Commands* in the *System Volume).* In addition:

- The CLI saves the commands in the format that you have input, that is, if you input a command in its incomplete form, the saved history command is also incomplete.
- If you execute a command for multiple times successively, the CLI saves the earliest one. However, if you execute the different forms of a command, the CLI saves each form of this command. For example, if you execute the **display cu** command for multiple times successively, the CLI saves only one history command; if you execute the **display cu** command and then the **display current-configuration** command, the CLI saves two history commands.

Follow these steps to access history commands:

| To do… | Use the key/command… | Result |
|---|---|---|
| View the history commands | **display history-command** | Displays the commands that you have entered |
| Access the previous history command | Up-arrow key or **Ctrl+P** | Displays the earlier history command, if there is any. |
| Access the next history command | Down-arrow key or **Ctrl+N** | Displays the next history command, if there is any. |

**Note**

You may use arrow keys to access history commands in Windows 200X and XP Terminal or Telnet. However, the up-arrow and down-arrow keys are invalid in Windows 9X HyperTerminal, because they are defined in a different way. You can press **Ctrl+P** or **Ctrl+N** instead.

## Command Line Error Information

The commands are executed only if they have no syntax error. Otherwise, error information is reported. Table 1-7 lists some common errors.

**Table 1-7** Common command line errors

| Error information | Cause |
|---|---|
| % Unrecognized command found at '^' position. | The command was not found. |
| | The keyword was not found. |
| | Parameter type error |
| | The parameter value is beyond the allowed range. |
| % Incomplete command found at '^' position. | Incomplete command |
| % Ambiguous command found at '^' position. | Ambiguous command, |
| Too many parameters | Too many parameters |
| % Wrong parameter found at '^' position. | Wrong parameter |

# Table of Contents

# 1 Device Management

When configuring device management, go to these sections for information you are interested in:



## Device Management Overview

Through the device management function, you can view the current working state of a device, configure running parameters, and perform daily device maintenance and management.

## Device Management Configuration Task List

Complete these tasks to configure device management:

| Task | Remarks |
|---|---|
| Configuring the Exception Handling Method | Optional |
| Rebooting a Device | Optional |
| Configuring the Scheduled Automatic Execution Function | Optional |
| Upgrading the Boot ROM Program Through Command Lines | Optional |
| Upgrading the Boot File Through Command Lines | Optional |
| Disabling Boot ROM Access | Optional |
| Configuring a Detection Interval | Optional |
| Clearing the 16-bit Interface Indexes Not Used in the Current System | Optional |
| Identifying and Diagnosing Pluggable Transceivers | Optional |

## Configuring the Exception Handling Method

When the system detects any software abnormality, it handles the situation with one of the following two methods:

- **reboot**: The system recovers itself through automatic reboot.

- **maintain**: The system maintains the current situation, and does not take any measure to recover itself. Therefore, you need to recover the system manually, such as reboot the system. Sometimes, it is difficult for the system to recover, or some prompts that are printed during the failure are lost after the reboot. In this case, you can use this method to maintain the abnormal state to locate problems and recover the system.

Follow these steps to configure the exception handling method:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the exception handling method | **system-failure** { **maintain** \| **reboot** } | Optional<br>By default, the system adopts the **reboot** method to handle exceptions. |

## Rebooting a Device

When a fault occurs to a running device, you can remove the fault by rebooting the device, depending on the actual situation.

You can reboot a device following any of the three methods:

- Power on the device after powering it off, which is also called hard reboot or cold start. This method impacts the device a lot. Powering off a running device will cause data loss and hardware damages. It is not recommended.
- Trigger the immediate reboot through command lines.
- Enable the scheduled reboot function through command lines. You can set a time at which the device can automatically reboot, or set a delay so that the device can automatically reboot within the delay.

The last two methods are command line operations. Reboot through command lines is also called hot start, which is equal to powering on the device after powering it off. It is mainly used to reboot a device in remote maintenance, without performing hardware reboot of the device.

Follow the step below to reboot a device through command lines immediately:

| To do… | Use the command… | Remarks |
|---|---|---|
| Reboot the system immediately | **reboot** | Required<br>Available in user view |

Follow these steps to reboot a device at a time through command lines:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the scheduled reboot function and specify a specific reboot time and date | **schedule reboot at** *hh:mm* [ *date* ] | Required<br>Use either approach.<br>The scheduled reboot function is disabled by default.<br>Available in user view. |
| Enable the scheduled reboot function and specify a reboot waiting time | **schedule reboot delay** { *hh:mm* \| *mm* } | |

**Caution**

- Device reboot may result in the interruption of the ongoing services. Use these commands with caution.
- Before device reboot, use the **save** command to save the current configurations. For details about the **save** command, refer to *File System Configuration* in the *System Volume*.
- Before device reboot, use the commands of **display startup** and **display boot-loader** to check if the configuration file and boot file for the next boot are configured. (For details about the **display startup** command, refer to *File System Configuration* in the *System Volume.*
- The precision of the rebooting timer is 1 minute. One minute before the rebooting time, the device will prompt “REBOOT IN ONE MINUTE” and will reboot in one minute.
- If a main boot file fails or does not exist, the device cannot be rebooted with the **reboot** command. In this case, you can re-specify a main boot file to reboot the device, or you can power off the device then power it on and the system automatically uses the backup boot file to restart the device.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

## Configuring the Scheduled Automatic Execution Function

The scheduled automatic execution function enables the system to automatically execute a specified command at a specified time in a specified view. This function is used for scheduled system upgrade or configuration.

Follow these steps to configure the scheduled automatic execution function:

| To do… | Use the command… | Remarks |
|---|---|---|
| Automatically execute the specified command at the specified time | **schedule job at** *time* [ *date* ] **view** *view command* | Optional<br>Use either command.<br>Available in user view. |
| Automatically execute the specified command after the specified delay | **schedule job delay** *time* **view** *view command* | |

Note that:

- At present, you can specify user view and system view only. To automatically execute the specified command in another view or automatically execute multiple commands at a time, you can configure the system to automatically execute a batch file at the specified time (note that you must provide a complete file path for the system to execute the batch file.).
- The system does not check the values of the *view* and *command* arguments. Therefore, ensure the correctness of the *command* argument (including the correct format of *command* and the correct relationship between the *command* and *view* arguments).
- After the specified automatic execution time is reached, the system executes the specified command in the background without displaying any information except system information such as log, trap and debug.
- The system does not require any interactive information when it is executing the specified command. If there is information for you to confirm, the system automatically inputs **Y** or **Yes**; if

characters need to be input, the system automatically inputs a default character string, or inputs an empty character string when there is no default character string.

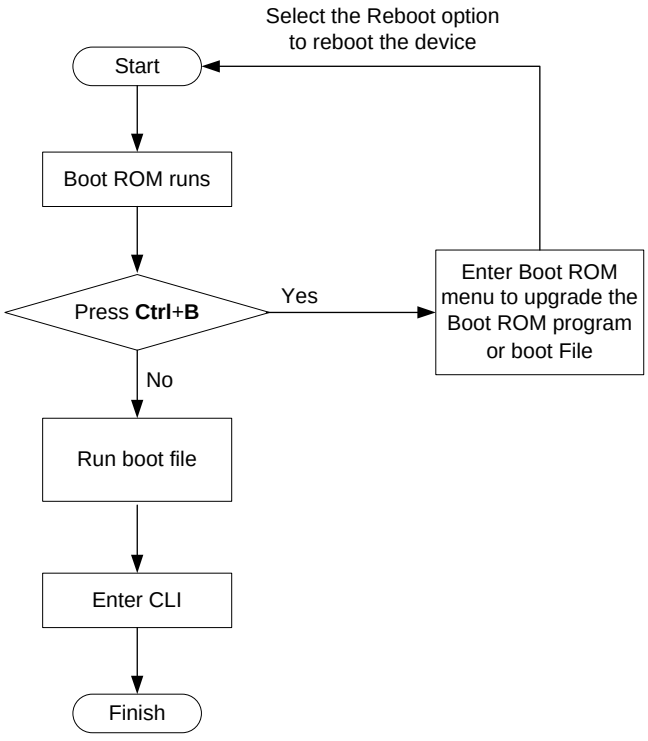
- For the commands used to switch user interfaces, such as **telnet**, **ftp**, and **ssh2**, the commands used to switch views, such as **system-view**, **quit**, and the commands used to modify status of a user that is executing commands, such as **super**, the operation interface, command view and status of the current user are not changed after the automatic execution function is performed.
- If the system time is modified after the automatic execution function is configured, the scheduled automatic execution configuration turns invalid automatically.
- Only the last configuration takes effect if you execute the **schedule job** command repeatedly.

# Upgrading Device Software

## Device Software Overview

Device software consists of the Boot ROM program and the system boot file. After the device is powered on, the Boot ROM program initialize the hardware, and display the hardware information. Then runs the boot file. The boot file provides hardware driver and adaptation for the system, and provides the support for the different functions. The Boot ROM program and system boot file are required for the startup and running of a device. Figure 1-1 illustrates their relationship.

**Figure 1-1** Relationship between the Boot ROM program and the system boot file




The Boot ROM program and system boot file can both be upgraded through the Boot ROM menu or command lines. The following sections describe the upgrading through command lines. For instructions about how to upgrade them through the Boot ROM menu, refer to the installation menu of your device.

## Upgrading the Boot ROM Program Through Command Lines

Follow these steps to upgrade the Boot ROM program:

1) Copy the Boot ROM program to the root directory of the device's storage medium using FTP or TFTP.

2) Upgrading the Boot ROM Program Through Command Lines.
3) Reboot the device to make the specified Boot ROM program take effect.

Follow these steps to upgrade the Boot ROM program:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the validity check function when upgrading the Boot ROM | **bootrom-update security-check enable** | Optional<br>By default, the validity check function is enabled at the time of upgrading Boot ROM. |
| Return to user view | **quit** | — |
| upgrade the Boot ROM program on devices | **bootrom update file** *file-url* | Required<br>Available in user view. |

### Upgrading the Boot File Through Command Lines

Follow the steps to upgrade the boot file:

1) Save the boot file to the root directory of the device's storage medium using FTP, TFTP, or other approaches.
2) Use a command to specify the boot file for the next boot of the device.
3) Reboot the device to make the boot file take effect.

Follow the step below to upgrade the boot file:

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify a boot file for the next boot | **boot-loader file** *file-url* { **main** \| **backup** } | Required<br>Available in user view. |

When multiple Boot ROM files are available on the storage media, you can specify a file for the next device boot by executing the following command. A main boot file is used to boot a device and a backup boot file is used to boot a device only when a main boot file is unavailable.

**Caution**

You must save the file for the next device boot under the root directory of the device. You can copy or move a file to change the path of it to the root directory.

## Disabling Boot ROM Access

By default, you can press **Ctrl+B** to enter the Boot ROM menu to configure the Boot ROM. However, this may bring security problems to the device. Therefore, the device provides the function of disabling the Boot ROM access to enhance security of the device. After this function is configured, no matter

whether you press **Ctrl+B** or not, the system does not enter the Boot ROM menu, but enters the command line configuration interface directly.

In addition, you need to set the Boot ROM access password when you enter the Boot ROM menu for the first time to protect the Boot ROM against operations of illegal users.

You can use the **display startup** command to view the status of the Boot ROM access function. For the detailed description of the **display startup** command, refer to *File System Management* in the *System Volume*.

Follow the step below to disable Boot ROM access:

| To do… | Use the command… | Remarks |
|---|---|---|
| Disable Boot ROM access | **undo startup bootrom-access enable** | Required<br>By default, Boot ROM access is enabled.<br>Available in user view. |

## Configuring a Detection Interval

When detecting an exception on a port, the operation, administration and maintenance (OAM) module will automatically shut down the port. The device will detect the status of the port when a detection interval elapses. If the port is still shut down, the device will recover it.

Follow these steps to configure a detection interval:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a detection interval | **shutdown-interval** *time* | Optional<br>The detection interval is 30 seconds by default. |

## Clearing the 16-bit Interface Indexes Not Used in the Current System

In practical networks, the network management software requires the device to provide a uniform, stable 16-bit interface index. That is, a one-to-one relationship should be kept between the interface name and the interface index in the same device.

For the purpose of the stability of an interface index, the system will save the 16-bit interface index when a logical interface is removed.

If you repeatedly insert and remove delete a large number of logical interfaces, the interface indexes will be used up, which will result in interface creation failures. To avoid such a case, you can clear all 16-bit interface indexes saved but not used in the current system in user view.

After the above operation,

- For a re-created interface, the new interface index may not be consistent with the original one.
- For existing interfaces, their interface indexes remain unchanged.

Follow these steps to clear the 16-bit interface indexes not used in the current system:

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear the 16-bit interface indexes saved but not used in the current system | **reset unused porttag** | Required<br>Available in user view. |

**Caution**

A confirmation is required when you execute this command. If you fail to make a confirmation within 30 seconds or enter **N** to cancel the operation, the command will not be executed.

# Identifying and Diagnosing Pluggable Transceivers

## Introduction to pluggable transceivers

At present, four types of pluggable transceivers are commonly used, as shown in Table 1-1. They can be further divided into optical transceivers and electrical transceivers based on transmission medium.

**Table 1-1** Commonly used pluggable transceivers

| Transceiver type | Application environment | Whether can be an optical transceiver | Whether can be an electrical transceiver |
|---|---|---|---|
| SFP (Small Form-factor Pluggable) | Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces | Yes | Yes |
| GBIC (Gigabit Interface Converter) | Generally used for 1000M Ethernet interfaces | Yes | Yes |
| XFP (10-Gigabit small Form-factor Pluggable) | Generally used for 10G Ethernet interfaces | Yes | No |
| XENPAK (10-Gigabit Ethernet Transceiver Package) | Generally used for 10G Ethernet interfaces | Yes | Yes |

## Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can use the following commands to view the key parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or name of the vendor who customizes the transceivers to identify the pluggable transceivers.

Follow these steps to identify pluggable transceivers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display key parameters of the pluggable transceiver(s) | **display transceiver interface** [ *interface-type interface-number* ] | Available for all pluggable transceivers. |
| Display part of the electrical label information of the anti-spoofing transceiver(s) customized by H3C | **display transceiver manuinfo interface** [ *interface-type interface-number* ] | Available for anti-spoofing pluggable transceiver(s) customized by H3C only. |

- You can use the **Vendor Name** field in the prompt information of the **display transceiver** command to identify an anti-spoofing pluggable transceiver customized by H3C. If the field is **H3C**, it is considered an H3C-customized pluggable transceiver.
- Electrical label information is also called permanent configuration data or archive information, which is written to the storage component of a board during device debugging or testing. The information includes name of the board, device serial number, and vendor name or name of the vendor who customizes the transceiver.

### Diagnosing pluggable transceivers

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. Optical transceivers customized by H3C also support the digital diagnosis function, which monitors the key parameters of a transceiver, such as temperature, voltage, laser bias current, TX power, and RX power. When these parameters are abnormal, you can take corresponding measures to prevent transceiver faults.

Follow these steps to diagnose pluggable transceivers:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current alarm information of the pluggable transceiver(s) | **display transceiver alarm interface** [ *interface-type interface-number* ] | Available for all pluggable transceivers. |
| Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by H3C | **display transceiver diagnosis interface** [ *interface-type interface-number* ] | Available for anti-spoofing pluggable optical transceiver(s) customized by H3C only. |

## Displaying and Maintaining Device Management Configuration

Follow these steps to display and maintain device management configuration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information of the boot file | **display boot-loader** | Available in any view |
| Display the statistics of the CPU usage | **display cpu-usage** [ *entry-number* [ *offset* ] [ **verbose** ] [ **from-device** ] ] | Available in any view |
| Display history statistics of the CPU usage in a chart | **display cpu-usage history** [ **task** *task-id* ] | Available in any view |
| Display information about hardware on the device | **display device** [ **subslot** *subslot-number* \| **verbose** ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display electrical label information of the device | **display device manuinfo** | Available in any view |
| Display the temperature information of devices | **display environment** | Available in any view |
| Display the operating state of fans in a device | **display fan** *fan-id* | Available in any view |
| Display the usage of the memory of a device | **display memory** | Available in any view |
| Display the power state of a device | **display power** [ *power-id* ] | Available in any view |
| Display state of the redundant power system (RPS) | **display rps** [ *rps-id* ] | Available in any view |
| Display the reboot type of a device | **display reboot-type** | Available in any view |
| Display the reboot time of a device | **display schedule reboot** | Available in any view |
| Display detailed configurations of the scheduled automatic execution function | **display schedule job** | Available in any view |
| Display the exception handling method | **display system-failure** | Available in any view |

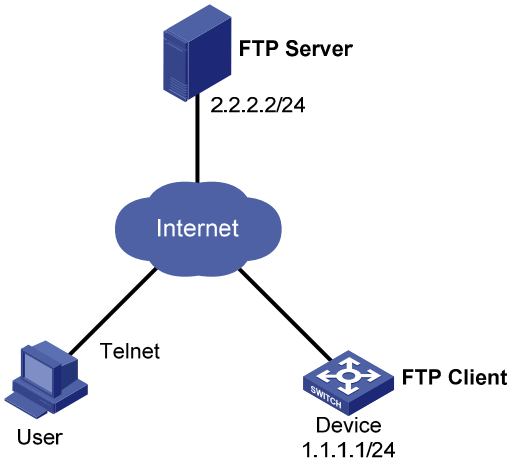
# Device Management Configuration Examples

## Remote Scheduled Automatic Upgrade Configuration Example

### Network requirement

- As shown in Figure 1-2, the current software version is **soft-version1** for Device. Upgrade the software version of Device to **soft-version2** and configuration file to **new-config** at a time when few services are processed (for example, at 3 am) through remote operations.
- The newest application **soft-version2.bin** and the newest configuration file **new-config.cfg** are both saved under the **aaa** directory of the FTP server.
- The IP address of Device is 1.1.1.1/24, the IP address of the FTP server is 2.2.2.2/24, and the FTP server is reachable.
- User can log in to Device via Telnet and a route exists between User and Device.

**Figure 1-2** Network diagram for remote scheduled automatic upgrade




## Configuration procedure

1) Configuration on the FTP server (Note that configurations may vary with different types of servers)

- Set the access parameters for the FTP client (including enabling the FTP server function, setting the FTP username to **aaa** and password to **hello**, and setting the user to have access to the **flash:/aaa** directory).

```
<FTP-Server> system-view
[FTP-Server] ftp server enable
[FTP-Server] local-user aaa
[FTP-Server-luser-aaa] password cipher hello
[FTP-Server-luser-aaa] service-type ftp
[FTP-Server-luser-aaa] authorization-attribute work-directory flash:/aaa
```

- Use text editor on the FTP server to edit batch file **auto-update.txt**. The following is the content of the batch file:

```
return
startup saved-configuration new-config.cfg
boot-loader file soft-version2.bin main
reboot
```

2) Configuration on Device

# Log in to the FTP server (note that the prompt may vary with servers.)

```
<Device> ftp 2.2.2.2
Trying 2.2.2.2 ...
Press CTRL+K to abort
Connected to 2.2.2.2.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(2.2.2.2:(none)):aaa
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

# Download file **auto-update.txt** on the FTP server.

```
[ftp] ascii
```

```
[ftp] get auto-update.txt
```

# Download file **new-config.cfg** on the FTP server.

```
[ftp]get new-config.cfg
```

# Download file **soft-version2.bin** on the FTP server.

```
[ftp] binary
[ftp] get soft-version2.bin
[ftp] bye
<Device>
```

# Modify the extension of file **auto-update.txt** as **.bat**.

```
<Device> rename auto-update.txt auto-update.bat
```

To ensure correctness of the file, you can use the **more** command to view the content of the file.

# Execute the scheduled automatic execution function to enable the device to be automatically upgraded at 3 am.

```
<Device> schedule job at 03:00 view system execute auto-update.bat
Info: Command execute auto-update.bat in system view will be executed at 03:00 12/11/2007(in
12 hours and  0 minutes).
```

After the device reboots, use the **display version** command to check if the upgrade is successful.

# Table of Contents

# 1 File System Management Configuration

When configuring file system management, go to these sections for information you are interested in:

- File System Management
- Configuration File Management
- Displaying and Maintaining Device Configuration

## File System Management

This section covers these topics:

- File System Overview
- Filename Formats
- Directory Operations
- File Operations
- Batch Operations
- Storage Medium Operations
- Setting File System Prompt Modes
- File System Operations Example

### File System Overview

A major function of the file system is to manage storage media. It allows you to perform operations such as directory create and delete, and file copy and display. If an operation, delete or overwrite for example, causes problems such as data loss or corruption, the file system will prompt you to confirm the operation by default.

Depending on the managed object, file system operations fall into Directory Operations, File Operations, Batch Operations, Storage Medium Operations, and Setting File System Prompt Modes.

### Filename Formats

When you specify a file, you must enter the filename in one of the following formats.

Filename formats:

| Format | Description | Length | Example |
|---|---|---|---|
| file-name | Specifies a file under the current working directory. | 1 to 91 characters | a.cfg: Indicates that a file named **a.cfg** is under the current working directory |
| path/file-name | Specifies a file in the specified folder under the current working directory. path indicates the name of the folder. You can specify multiple folders, indicating a file under a multi-level folder. | 1 to 135 characters | test/a.cfg: Indicates that a file named **a.cfg** is in the **test** folder under the current working directory. |

| Format | Description | Length | Example |
|---|---|---|---|
| drive:/[path]/file-name | Specifies a file in the specified storage medium on the device. drive represents the storage medium name. The 3Com Switch 4500G use flashes as their storage media. | 1 to 135 characters | flash:/test/a.cfg: Indicates that a file named **a.cfg** is in the **test** folder under the root directory of the flash memory. |

## Directory Operations

Directory operations include creating/removing a directory, displaying the current working directory, displaying the specified directory or file information, and so on.

### Displaying directory information

| To do… | Use the command… | Remarks |
|---|---|---|
| Display directory or file information | **dir** [ /**all** ] [ *file-url* ] | Required<br>Available in user view |

### Displaying the current working directory

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current working directory | **pwd** | Required<br>Available in user view |

### Changing the current working directory

| To do… | Use the command… | Remarks |
|---|---|---|
| Change the current working directory | **cd** { *directory* \| **..** \| **/** } | Required<br>Available in user view |

### Creating a directory

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a directory | **mkdir** *directory* | Required<br>Available in user view |

### Removing a directory

| To do… | Use the command… | Remarks |
|---|---|---|
| Remove a directory | **rmdir** *directory* | Required<br>Available in user view |

Note

- The directory to be removed must be empty, meaning that before you remove a directory, you must delete all the files and the subdirectory under this directory. For file deletion, refer to the **delete** command; for subdirectory deletion, refer to the **rmdir** command.
- After you execute the **rmdir** command successfully, the files in the recycle bin under the directory will be automatically deleted.

## File Operations

File operations include displaying the specified directory or file information; displaying file contents; renaming, copying, moving, removing, restoring, and deleting files.

Note

You can create a file by copying, downloading or using the **save** command.

### Displaying file information

| To do… | Use the command… | Remarks |
|---|---|---|
| Display file or directory information | **dir** [ /**all** ] [ *file-url* ] | Required<br>Available in user view |

### Displaying the contents of a file

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the contents of a file | **more** *file-url* | Required<br>Currently only a .txt file can be displayed.<br>Available in user view |

### Renaming a file

| To do… | Use the command… | Remarks |
|---|---|---|
| Rename a file | **rename** *fileurl-source fileurl-dest* | Required<br>Available in user view |

### Copying a file

| To do… | Use the command… | Remarks |
|---|---|---|
| Copy a file | **copy** *fileurl-source fileurl-dest* | Required<br>Available in user view |

### Moving a file

| To do… | Use the command… | Remarks |
|---|---|---|
| Move a file | **move** *fileurl-source fileurl-dest* | Required<br>Available in user view |

### Deleting a file

| To do… | Use the command… | Remarks |
|---|---|---|
| Move a file to the recycle bin or delete it permanently | **delete** [ **/unreserved** ] *file-url* | Required<br>Available in user view |

**Caution**

- The files in the recycle bin still occupy storage space. To delete a file in the recycle bin, you need to execute the **reset recycle-bin** command in the directory that the file originally belongs. It is recommended to empty the recycle bin timely with the **reset recycle-bin** command to save storage space.
- The **delete /unreserved** *file-url* command deletes a file permanently and the action cannot be undone. Execution of this command equals that you execute the **delete** *file-url* command and then the **reset recycle-bin** command in the same directory.

### Restoring a file from the recycle bin

| To do… | Use the command… | Remarks |
|---|---|---|
| Restore a file from the recycle bin | **undelete** *file-url* | Required<br>Available in user view |

### Emptying the recycle bin

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter the original working directory of the file to be deleted | **cd** { *directory* \| **..** \| **/** } | Optional<br>If the original directory of the file to be deleted is not the current working directory, this command is required.<br>Available in user view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Delete the file under the current directory and in the recycle bin | **reset recycle-bin** [ **/force** ] | Required<br>Available in user view |

## Batch Operations

A batch file is a set of executable commands. Executing a batch file equals executing the commands in the batch file one by one.

The following steps are recommended to execute a batch file:

1) Edit the batch file on your PC.
2) Download the batch file to the device. If the suffix of the file is not **.bat**, use the **rename** command to change the suffix to **.bat**.
3) Execute the batch file.

Follow the steps below to execute a batch file:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Execute a batch file | **execute** *filename* | Required |

**Caution**

Execution of a batch file does not guarantee the successful execution of every command in the batch file. If a command has error settings or the conditions for executing the command are not satisfied, the system will skip the command to the next one.

## Storage Medium Operations

### Managing space of the storage medium

When some space of a storage medium becomes inaccessible due to abnormal operations for example, you can use the **fixdisk** command to restore the space of the storage medium. The execution of the **format** command will format the storage medium, and all the data on the storage medium will be deleted.

Use the following commands to manage the storage medium space:

| To do… | Use the command… | Remarks |
|---|---|---|
| Restore the space of a storage medium | **fixdisk** *device* | Optional<br>Available in user view |
| Format a storage medium | **format** *device* | Optional<br>Available in user view |

**Caution**

When you format a storage medium, all the files stored on it are erased and cannot be restored. In particular, if there is a startup configuration file on the storage medium, formatting the storage medium results in loss of the startup configuration file.

## Setting File System Prompt Modes

The file system provides the following two prompt modes:

- **alert**: In this mode, the system warns you about operations that may bring undesirable consequences such as file corruption or data loss.
- **quiet**: In this mode, the system does not prompt confirmation for any operation.

To prevent undesirable consequence resulting from misoperations, the **alert** mode is preferred.

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the operation prompt mode of the file system | **file prompt** { **alert** \| **quiet** } | Optional<br>The default is **alert**. |

## File System Operations Example

# Display the files and the subdirectories under the current directory.

```
<Sysname> dir
Directory of flash:/

   0   drw-         -  Feb 16 2006 11:45:36   logfile
   1   -rw-      1218  Feb 16 2006 11:46:19   config.cfg
   2   drw-         -  Feb 16 2006 15:20:27   test
   3   -rw-    8066003  Feb 16 2006 15:30:20   aaa.bin

15240 KB total (2521 KB free)
```

# Create a new folder called **mytest** under the test directory.

```
<Sysname> cd test
<Sysname> mkdir mytest
%Created dir flash:/test/mytest.
```

# Display the current working directory.

```
<Sysname> pwd
flash:/test
```

# Display the files and the subdirectories under the test directory.

```
<Sysname> dir
Directory of flash:/test/
```

```
   0   drw-         -  Feb 16 2006 15:28:14   mytest

15240 KB total (2521 KB free)
```

# Return to the upper directory.

```
<Sysname> cd ..
```

# Display the current working directory.

```
<Sysname> pwd
flash:
```

# Configuration File Management

The device provides the configuration file management function with a user-friendly command line interface (CLI) for you to manage the configuration files conveniently.

This section covers these topics:



## Configuration File Overview

A configuration file saves the device configurations in command lines in text format. You can view configuration information conveniently through configuration files.

### Types of configuration

The configuration of a device falls into two types:

- Startup configuration, a configuration file used for initialization when the device boots. If this file does not exist, the system boots using null configuration, that is, using the default parameters.
- Current configuration, which refers to the currently running configuration of the system. The current configuration may include the startup configuration if the startup configuration is not modified during system operation, and it also includes the new configuration added during the system operation. The current configuration is stored in the temporary storage medium of the device, and will be removed when the device reboots if not saved.

### Format and content of a configuration file

A configuration file is saved as a text file. It is saved following these rules:

- The content of a configuration file is command lines, and only non-default configuration settings are saved.
- Commands in a configuration file are listed in sections by views, usually in the order of system view, interface view, routing protocol view, and user interface view. Sections are separated with one or multiple blank lines or comment lines that start with a pound sign #.
- Ends with a return.

### Coexistence of multiple configuration files

Multiple configuration files can be stored on a storage medium of a device. You can save the configuration used in different environments as different configuration files. In this case, when the device moves between these networking environments, you just need to specify the corresponding configuration file as the startup configuration file for the next boot of the device and restart the device, so that the device can adapt to the network rapidly, saving the configuration workload.

A device boots using only one configuration file. However, you can specify two startup configuration files, main and backup startup configuration file, for the next startup of the device as needed and when the device supports this feature. When the device boots, the system uses the main startup configuration file, and if the main startup configuration file is corrupted or lost, the system will use the backup startup configuration file for device boot and configuration. The devices supporting the configuration of the main and backup startup configuration files, compared with the devices that do not support this feature, are more secure and reliable.

At a moment, there are at most one main startup configuration file and one backup startup configuration file. You can specify neither of the two files (displayed as NULL), or specify the two files as the same configuration file.

You can specify the main and backup startup configuration files for the next boot of the device in the following two methods:

- Specify them when saving the current configuration. For detailed configuration, refer to Saving the Current Configuration.
- Specify them when specifying the startup configuration file for the next system startup. For detailed configuration, refer to Specifying a Startup Configuration File for the Next System Startup.

### Startup with the configuration file

The device takes the following steps when it boots:

1) If the main startup configuration file exists, the device initializes with this configuration file.
2) If the main startup configuration file does not exist but the backup startup configuration file exists, the device initializes with the backup startup configuration file.
3) If neither the main nor the backup startup configuration file exists, the device will boot with null configuration (boot with null configuration means to boot with the factory default configuration).

## Saving the Current Configuration

### Introduction

You can modify the current configuration on your device using command line interface. However, the current configuration is temporary. To make the modified configuration take effect at the next boot of the device, you must save the current configuration to the startup configuration file before the device reboots.

### Modes in saving the configuration

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file more quickly but is likely to lose the existing configuration file if the device reboots or the power fails during the process.
- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file more slowly but can retain the configuration file in the device even if the device reboots or the power fails during the process.

The fast saving mode is suitable for environments where power supply is stable. The safe mode, however, is preferred in environments where stable power supply is unavailable or remote maintenance is involved.

Follow the steps below to save the current configuration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Save the current configuration to the specified file, but the configuration file will not be set as the file for the next startup | **save** *file-url* | Required<br>Available in any view |
| Save the current configuration to the root directory of the storage medium and specify the file as the startup configuration file that will be used at the next system startup | **save** [ **safely** ] [ **backup** \| **main** ] | |

**Note**

- The configuration file must be with extension **.cfg**.
- For the device that supports the **main** keyword, the execution of the **save** [ **safely** ] and **save** [ **safely** ] **main** commands has the same effect: The system will save the current configuration and specify the configuration file as the main startup configuration file to be used at the next system startup.
- During the execution of the **save** [ **safely** ] [ **backup** | **main** ] command, the startup configuration file to be used at the next system startup may be lost if the device reboots or the power supply fails. In this case, the device will boot with the null configuration, and after the device reboots, you need to re-specify a startup configuration file for the next system startup (refer to Specifying a Startup Configuration File for the Next System Startup).

## Specifying a Startup Configuration File for the Next System Startup

A startup configuration file is the configuration file to be used at the next system startup. You can specify a configuration file as the startup configuration file to be used at the next system startup in the following two ways:

- Use the **save** command. If you save the current configuration to the specified configuration file in the interactive mode, the system automatically sets the file as the main configuration file to be used at the next system startup.
- Use the command dedicated to specify a startup configuration file, which is described in the following table:

Follow the step below to specify a configuration file as the startup configuration file for the next system startup:

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify a startup configuration file for the next system startup | **startup saved-configuration** *cfgfile* [ **backup** \| **main** ] | Required<br>Available in user view |

**Caution**

A configuration file must use **.cfg** as its extension name and the startup configuration file must be saved under the root directory of the storage medium.

## Backing Up the Startup Configuration File

The backup function allows you to copy the startup configuration file to be used at the next system startup from the device to the TFTP server for backup.

The backup operation backs up the startup configuration file to the TFTP server for devices supporting main/backup startup configuration file.

Follow the step below to back up the startup configuration file to be used at the next system startup:

| To do… | Use the command… | Remarks |
|---|---|---|
| Back up the configuration file to be used at the next system startup to the specified TFTP server | **backup startup-configuration to** *dest-addr* [*dest- filename* ] | Required<br>Available in user view |

**Note**

Before the backup operation, you should:

- Ensure that the server is reachable, the server is enabled with TFTP service, and the client has permission to read and write.
- Use the **display startup** command (in user view) to see whether you have set the startup configuration file, and use the **dir** command to see whether this file exists. If the file is set as NULL or does not exist, the backup operation will fail.

## Deleting the Startup Configuration File for the Next Startup

You can delete the startup configuration file to be used at the next system startup using commands. You can choose to delete either the main or backup startup configuration file. However, in the case that the main and backup startup configuration files are the same, if you perform the delete operation for once, the system will not delete the configuration file but only set the corresponding startup configuration file (main or backup, according to which one you specified in the command) to NULL.

You may need to delete the startup configuration file for the next startup for one of these reasons:

- After you upgrade system software, the existing configuration file does not match the new system software.
- The configuration file is corrupted (often caused by loading a wrong configuration file).

After the startup configuration file is deleted, the system will use the null configuration when the device reboots.

Follow the step below to delete the startup configuration file for the next startup:

| To do… | Use the command… | Remarks |
|---|---|---|
| Delete the startup configuration file for the next startup from the storage medium | **reset saved-configuration** [ **backup** \| **main** ] | Required<br>Available in user view |

**Caution**

This command will permanently delete the configuration file from the device. Use it with caution.

### Restoring the Startup Configuration File

The restore function allows you to copy a configuration file from TFTP server to the device and specify the file as the startup configuration file to be used at the next system startup.

Follow the step below to restore the startup configuration file to be used at the next system startup:

| To do… | Use the command… | Remarks |
|---|---|---|
| Restore the startup configuration file to be used at the next system startup | **restore startup-configuration from** *src-addr src-filename* | Required<br>Available in user view |

**Note**

- The restore operation restores the main startup configuration file.
- Before restoring a configuration file, you should ensure that the server is reachable, the server is enabled with TFTP service, and the client has read and write permission.
- After the command is successfully executed, you can use the **display startup** command (in user view) to verify that the filename of the configuration file to be used at the next system startup is the same with that specified by the *filename* argument, and use the **dir** command to verify that the restored startup configuration file exists.

## Displaying and Maintaining Device Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the currently running configuration file saved on the storage medium of the device | **display saved-configuration** [ **by-linenum** ] | Available in any view |
| Display the configuration files for this and the next system startup | **display startup** | Available in any view |
| Display the validated configuration in current view | **display this** [ **by-linenum** ] | Available in any view |

| To do… | Use the command… | Remarks |
| --- | --- | --- |
| Display the current configuration | **display current-configuration** [ [ **configuration** [ *configuration* ] \| **interface** [ *interface-type* ] [ *interface-number* ] ] [ **by-linenum** ] [ **\|** { **begin** \| **include** \| **exclude** } *text* ] ] | Available in any view |

# 2 FTP Configuration

When configuring FTP, go to these sections for information you are interested in:



## FTP Overview

### Introduction to FTP

The File Transfer Protocol (FTP) is an application layer protocol for sharing files between server and client over a TCP/IP network.

FTP uses TCP ports 20 and 21 for file transfer. Port 20 is used to transmit data, and port 21 to transmit control commands. Refer to RFC 959 for details of FTP basic operation.

FTP transfers files in two modes:

- Binary mode for program file transmission, like files with the suffixes **.app**, **.bin**, or **.btm.**
- ASCII mode for text file transmission, like files with the suffixes **.txt**, **.bat**, or **.cfg**.

### Operation of FTP

FTP adopts the client/server model. Your device can function either as the client or as the server (as shown in Figure 2-1).

- When the device serves as the FTP client, the user first connects to the device from a PC through Telnet or an emulation program, and then executes the **ftp** command to establish a connection to the remote FTP server and gain access to the files on the server.
- When the device serves as the FTP server, FTP clients (users running the FTP client program) log in to the device to access files on the device (the administrator must configure the IP address of the device as the FTP server IP address before user login).

**Figure 2-1** Network diagram for FTP


When the device serves as the FTP client, you need to perform the following configuration:

**Table 2-1** Configuration when the device serves as the FTP client

| Device | Configuration | Remarks |
|---|---|---|
| Device (FTP client) | Use the **ftp** command to establish the connection to the remote FTP server | If the remote FTP server supports anonymous FTP, the device can log in to it directly; if not, the device must obtain the FTP username and password first to log in to the remote FTP server. |
| PC (FTP server) | Enable FTP server on the PC, and configure the username, password, user privilege level, and so on. | — |

When the device serves as the FTP server, you need to perform the following configuration:

**Table 2-2** Configuration when the device serves as the FTP server

| Device | Configuration | Remarks |
|---|---|---|
| Device (FTP server) | Enable the FTP server function | Disabled by default.<br>You can use the **display ftp-server** command to view the FTP server configuration on the device. |
| | Configure authentication and authorization | Configure the username, password, authorized working directory for an FTP user.<br>The device does not support anonymous FTP for security reasons. Therefore, you must use a valid username and password. By default, authenticated users can access the root directory of the device. |
| | Configure the FTP server operating parameters | Parameters such as the FTP connection timeout time |
| PC (FTP client) | Use the FTP client program to log in to the FTP server. | You can log in to the FTP server only after you input the correct FTP username and password. |

**Caution**

- The FTP function is available when a reachable route exists between the FTP server and the FTP client.
- When you use IE to log in to the device serving as the FTP server, part of the FTP functions is not available. This is because multiple connections are established during the login process but the device supports only one connection at a time.

# Configuring the FTP Client

## Establishing an FTP Connection

To access an FTP server, an FTP client must establish a connection with the FTP server. Two ways are available to establish a connection: using the **ftp** command to establish the connection directly; using the **open** command in FTP client view.

Source address binding means to configure an IP address on a stable interface such as a loopback interface, and then use this IP address as the source IP address of an FTP connection. The source address binding function simplifies the configuration of ACL rules and security policies. You just need to specify the source or destination address argument in an ACL rule as this address to filter inbound and outbound packets on the device, ignoring the difference between interface IP addresses as well as the affect of interface statuses. You can configure the source address by configuring the source interface or source IP address. The primary IP address configured on the source interface is the source address of the transmitted packets. The source address of the transmitted packets is selected following these rules:

- If no source address is specified, the FTP client uses the IP address of the interface determined by the matched route as the source IP address to communicate with an FTP server.
- If the source address is specified with the **ftp client source** or **ftp** command, this source address is used to communicate with an FTP server.
- If you use the **ftp client source** command and the **ftp** command to specify a source address respectively, the source address specified with the **ftp** command is used to communicate with an FTP server.

The source address specified with the **ftp client source** command is valid for all FTP connections and the source address specified with the **ftp** command is valid only for the current FTP connection.

Follow these steps to establish an FTP connection (In IPv4 networking):

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the source address of the FTP client | **ftp client source** { **interface** *interface-type interface-number* \| **ip** *source-ip-address* } | Optional<br>A device uses the IP address of the interface determined by the matched route as the source IP address to communicate with the FTP server by default. |
| Exit to system view | **quit** | — |
| Log in to the remote FTP server directly in user view | **ftp** [ *server-address* [ *service-port* ] [ **source** { **interface** *interface-type interface-number* \| **ip** *source-ip-address* } ] ] | Use either approach.<br>The **ftp** command is available in user view; and the **open** command is available in FTP client view. |
| Log in to the remote FTP server indirectly in FTP client view | **ftp** | |
| | **open** *server-address* [ *service-port* ] | |

**Note**

- If no primary IP address is configured on the specified source interface, no FTP connection can be established.
- If you use the **ftp client source** command to first configure the source interface and then the source IP address of the transmitted packets, the newly configured source IP address will take effect instead of the current source interface, and vice versa.

Follow these steps to establish an FTP connection (In IPv6 networking):

| To do… | Use the command… | Remarks |
|---|---|---|
| Log in to the remote FTP server directly in user view | **ftp ipv6** [ *server-address* [ *service-port* ] [ **source ipv6** *source-ipv6-address* ] [ **-i** *interface-type interface-number* ] ] | Use either approach.<br>The **ftp ipv6** command is available in user view; and the **open ipv6** command is available in FTP client view. |
| Log in to the remote FTP server indirectly in FTP client view | **ftp ipv6** | |
| | **open ipv6** *server-address* [ *service-port* ] [ **-i** *interface-type interface-number* ] | |

## Configuring the FTP Client

After a device serving as the FTP client has established a connection with the FTP server (For how to establish an FTP connection, refer to Establishing an FTP Connection.), you can perform the following operations in the authorized directories of the FTP server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Display help information of FTP-related commands supported by the remote FTP server | **remotehelp** [ *protocol-command* ] | Optional |
| Enable information display in a detailed manner | **verbose** | Optional<br>Enabled by default |
| Enable FTP related debugging when the device acts as the FTP client | **debugging** | Optional<br>Disabled by default |
| Use another username to relog after logging in to the FTP server successfully | **user** *username* [ *password* ] | Optional |
| Set the file transfer mode to ASCII | **ascii** | Optional<br>ASCII by default |
| Set the file transfer mode to binary | **binary** | Optional<br>ASCII by default |
| Change the working path on the remote FTP server | **cd** { *directory* \| **..** \| **/** } | Optional |

| To do… | Use the command… | Remarks |
|---|---|---|
| Exit the current directory and enter the upper level directory | **cdup** | Optional |
| View the detailed information of the files/directories on the FTP server | **dir** [ *remotefile* [ *localfile* ] ] | Optional |
| View the names of the files/directories on the FTP server | **ls** [ *remotefile* [ *localfile* ] ] | Optional |
| Download a file from the FTP server | **get** *remotefile* [ *localfile* ] | Optional |
| Upload a file to the FTP server | **put** *localfile* [ *remotefile* ] | Optional |
| View the currently accessed directory on the remote FTP server | **pwd** | Optional |
| View the working directory of the FTP client | **lcd** | Optional |
| Create a directory on the FTP server | **mkdir** *directory* | Optional |
| Set the data transfer mode to passive | **passive** | Optional<br>Passive by default |
| Permanently delete the specified file on the FTP server | **delete** *remotefile* | Optional |
| Delete specified directory on the FTP server | **rmdir** *directory* | Optional |
| Disconnect from the FTP server without exiting the FTP client view | **disconnect** | Optional<br>Equal to the **close** command |
| Disconnect from the FTP server without exiting the FTP client view | **close** | Optional<br>Equal to the **disconnect** command |
| Disconnect from the FTP server and exit to user view | **bye** | Optional |
| Terminate the connection with the remote FTP server, and exit to user view | **quit** | Optional<br>Available in FTP client view, equal to the **bye** command |

**Note**

- FTP uses two modes for file transfer: ASCII mode and binary mode.
- The **ls** command can only display the file/directory name, while the **dir** command can display more information, such as the sizes of and date of creation of files or directories.
- The commands listed in the above table are only available for level 3 (manage level) users logging in to the device which serves as the FTP client. However, whether the users can successfully execute the commands depends on the FTP server's authorization.

## FTP Client Configuration Example

### Network requirements

- As shown in Figure 2-2, use Device as an FTP client and PC as the FTP server. Their IP addresses are 10.2.1.1/16 and 10.1.1.1/16 respectively. An available route exists between Device and PC.
- Device downloads a startup file from PC for device upgrade, and uploads the configuration file to PC for backup.
- On PC, an FTP user account has been created for the FTP client, with the username being **abc** and the password being **pwd**.

**Figure 2-2** Network diagram for FTPing a startup file from an FTP server


### Configuration procedure

---

**Caution**

If the available memory space of the device is not enough, use the **fixdisk** command to clear the memory or use the **delete /unreserved** *file-url* command to delete the files not in use and then perform the following operations.

---

# Log in to the server through FTP.

```
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1
Connected to 10.1.1.1
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(10.1.1.1:(none)):abc
331 Give me your password, please
Password:
230 Logged in successfully
```

# Set the file transmission mode to binary to transmit startup file.

```
[ftp] binary
200 Type set to I.
```

# Download the startup file **newest.bin** from PC to Device.

```
[ftp] get newest.bin
```

# Upload the configuration file **config.cfg** of Device to the server for backup.

```
[ftp] ascii
[ftp] put config.cfg back-config.cfg
227 Entering Passive Mode (10,1,1,1,4,2).
125 ASCII mode data connection already open, transfer starting for /config.cfg.
```

```
226 Transfer complete.
FTP: 3494 byte(s) sent in 5.646 second(s), 618.00 byte(s)/sec.
[ftp] bye
```

# Specify **newest.bin** as the main startup file to be used at the next startup.

```
<Sysname> boot-loader file newest.bin main
```

# Reboot the device, and the startup file is updated at the system reboot.

```
<Sysname> reboot
```

**Caution**

The startup file used for the next startup must be saved under the root directory of the storage medium . You can copy or move a file to the root directory of the storage medium. For the details of the **boot-loader** command, refer to *Device Management Commands* in the *System Volume*.

# Configuring the FTP Server

## Configuring FTP Server Operating Parameters

The FTP server uses one of the two modes to update a file when you upload the file (use the **put** command) to the FTP server:

- In fast mode, the FTP server starts writing data to the storage medium after a file is transferred to the memory. This prevents the existing file on the FTP server from being corrupted in the event that anomaly, power failure for example, occurs during a file transfer.
- In normal mode, the FTP server writes data to the storage medium while receiving data. This means that any anomaly, power failure for example, during file transfer might result in file corruption on the FTP server. This mode, however, consumes less memory space than the fast mode.

Follow these steps to configure the FTP server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the FTP server | **ftp server enable** | Required<br>Disabled by default. |
| Use an ACL to control FTP clients' access to the device | **ftp server acl** *acl-number* | Optional<br>By default, no ACL is used to control FTP clients' access to the device. |
| Configure the idle-timeout timer | **ftp timeout** *minutes* | Optional<br>30 minutes by default.<br>Within the idle-timeout time, if there is no information interaction between the FTP server and client, the connection between them is terminated. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the file update mode for the FTP server | **ftp update** { **fast** \| **normal** } | Optional<br>Normal update is used by default. |
| Quit to user view | **quit** | — |
| Manually release the FTP connection established with the specified username | **free ftp user** *username* | Optional<br>Available in user view |

## Configuring Authentication and Authorization on the FTP Server

To allow an FTP user to access certain directories on the FTP server, you need to create an account for the user, authorizing access to the directories and associating the username and password with the account.

The following configuration is used when the FTP server authenticates and authorizes a local FTP user. If the FTP server needs to authenticate a remote FTP user, you need to configure authentication, authorization and accounting (AAA) policy instead of the local user. For detailed configuration, refer to *AAA Configuration* in the *Security Volume*.

Follow these steps to configure authentication and authorization for FTP server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a local user and enter its view | **local-user** *user-name* | Required<br>No local user exists by default, and the system does not support FTP anonymous user access. |
| Assign a password to the user | **password** { **simple** \| **cipher** } *password* | Required |
| Assign the FTP service to the user | **service-type ftp** | Required<br>By default, the system does not support anonymous FTP access, and does not assign any service. If the FTP service is assigned, the root directory of the device is used by default. |
| Configure user properties | **authorization-attribute** { **acl** *acl-number* \| **callback-number** *callback-number* \| **idle-cut** *minute* \| **level** *level* \| **user-profile** *profile-name* \| **vlan** *vlan-id* \| **work-directory** *directory-name* } * | Optional<br>By default, the FTP/SFTP users can access the root directory of the device, and the user level is 0. You can change the default configuration by using this command. |

**Note**

- For more information about the **local-user**, **password**, **service-type ftp**, and **authorization-attribute** commands, refer to *AAA Commands* in the *Security Volume*.
- When the device serves as the FTP server, if the client is to perform the write operations (upload, delete, create, and delete for example) on the device's file system, the FTP login users must be level 3 users; if the client is to perform other operations, for example, read operation, the device has no restriction on the user level of the FTP login users, that is, any level from 0 to 3 is allowed.

## FTP Server Configuration Example

### Network requirements

- As shown in Figure 2-3, use Device as an FTP server, and the PC as the FTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. An available route exists between Device and PC.
- PC keeps the updated startup file of the device. Use FTP to upgrade the device and back up the configuration file.
- Set the username to **ftp** and the password to **pwd** for the FTP client to log in to the FTP server.

**Figure 2-3** Upgrading using the FTP server


### Configuration procedure

1) Configure Device (FTP Server)

# Create an FTP user account **ftp**, set its password to **pwd** and the user privilege level to level 3 (the manage level). Authorize **ftp**'s access to the root directory of the flash, and specify **ftp** to use FTP.

```
<Sysname> system-view
[Sysname] local-user ftp
[Sysname-luser-ftp] password simple pwd
[Sysname-luser-ftp] authorization-attribute work-directory level 3
[Sysname-luser-ftp] authorization-attribute work-directory flash:/
[Sysname-luser-ftp] service-type ftp
[Sysname-luser-ftp] quit
```

# Enable FTP server.

```
[Sysname] ftp server enable
[Sysname] quit
```

# Check files on your device. Remove those redundant to ensure adequate space for the startup file to be uploaded.

```
<Sysname> dir
Directory of flash:/
```

```
   0   drw-         -  Dec 07 2005 10:00:57   filename
   1   drw-         -  Jan 02 2006 14:27:51   logfile
   2   -rw-      1216  Jan 02 2006 14:28:59   config.cfg
   3   -rw-      1216  Jan 02 2006 16:27:26   back.cfg

15240 KB total (2511 KB free)
<Sysname> delete /unreserved flash:/back.cfg
```

2) Configure the PC (FTP Client)

# Log in to the FTP server through FTP.

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

# Download the configuration file **config.cfg** of the device to the PC for backup.

```
ftp> get config.cfg back-config.cfg
```

# Upload the configuration file **newest.bin** to Device.

```
ftp> put newest.bin
ftp> bye
```

---

**Note**

- You can take the same steps to upgrade configuration file with FTP. When upgrading the configuration file with FTP, put the new file under the root directory of the storage medium.
- After you finish upgrading the Boot ROM program through FTP, you must execute the **bootrom update** command to upgrade the Boot ROM.

---

3) Upgrade Device

# Specify **newest.bin** as the main startup file to be used at the next startup.

```
<Sysname> boot-loader file newest.bin main
```

# Reboot the device and the startup file is updated at the system reboot.

```
<Sysname> reboot
```

---

**Caution**

The startup file used for the next startup must be saved under the root directory of the storage medium. You can copy or move a file to the root directory of the storage medium. For the details of the **boot-loader** command, refer to *Device Management Commands* in the *System Volume*.

---

## Displaying and Maintaining FTP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration of the FTP client | **display ftp client configuration** | Available in any view |
| Display the configuration of the FTP server | **display ftp-server** | Available in any view |
| Display detailed information about logged-in FTP users | **display ftp-user** | Available in any view |

# 3 TFTP Configuration

When configuring TFTP, go to these sections for information you are interested in:



## TFTP Overview

### Introduction to TFTP

The Trivial File Transfer Protocol (TFTP) provides functions similar to those provided by FTP, but it is less complex than FTP in interactive access interface and authentication. Therefore, it is more suitable in environments where complex interaction is not needed between client and server.

TFTP uses the UDP port 69 for data transmission. For TFTP basic operation, refer to RFC 1986.

In TFTP, file transfer is initiated by the client.

- In a normal file downloading process, the client sends a read request to the TFTP server, receives data from the server, and then sends the acknowledgement to the server.
- In a normal file uploading process, the client sends a write request to the TFTP server, sends data to the server, and receives the acknowledgement from the server.

TFTP transfers files in two modes:

- Binary mode for program file transmission, like files with the suffixes **.app**, **.bin**, or **.btm**.
- ASCII mode for text file transmission, like files with the suffixes **.txt**, **.bat**, or **.cfg**.

### Operation of TFTP

**Note**

Only the TFTP client service is available with your device at present.

**Figure 3-1** TFTP configuration diagram


Before using TFTP, the administrator needs to configure IP addresses for the TFTP client and server, and make sure that there is a reachable route between the TFTP client and server.

When the device serves as the TFTP client, you need to perform the following configuration:

**Table 3-1** Configuration when the device serves as the TFTP client

| Device | Configuration | Remarks |
|---|---|---|
| Device (TFTP client) | • Configure the IP address and routing function, and ensure that the route between the device and the TFTP server is available.<br>• Use the **tftp** command to establish a connection to the remote TFTP server to upload/download files to/from the TFTP server | — |
| PC (TFTP server) | Enable TFTP server on the PC, and configure the TFTP working directory. | — |

## Configuring the TFTP Client

When a device acts as a TFTP client, you can upload a file on the device to a TFTP server and download a file from the TFTP server to the local device. You can use either of the following ways to download a file:

- Normal download: The device writes the obtained file to the storage medium directly. In this way, if you use a filename that exists in the directory, the original system file will be overwritten and if file download fails (for example, due to network disconnection), the device cannot start up normally because the original system file has been deleted.
- Secure download: The device saves the obtained file to its memory and does not write it to the storage medium until the whole file is obtained. In this way, if file download fails (for example, due to network disconnection), the device can still start up because the original system file is not overwritten. This mode is more secure but consumes more memory.

You are recommended to use the secure mode or, if you use the normal mode, specify a filename not existing in the current directory as the target filename when downloading the startup file or the startup configuration file.

Source address binding means to configure an IP address on a stable interface such as a loopback interface, and then use this IP address as the source IP address of a TFTP connection. The source address binding function simplifies the configuration of ACL rules and security policies. You just need to specify the source or destination address argument in an ACL rule as this address to filter inbound and outbound packets on the device, ignoring the difference between interface IP addresses as well as the affect of interface statuses. You can configure the source address by configuring the source interface or source IP address. The primary IP address configured on the source interface is the source address of the transmitted packets. The source address of the transmitted packets is selected following these rules:

- If no source address of the TFTP client is specified, a device uses the IP address of the interface determined by the matched route as the source IP address to communicate with a TFTP server.
- If the source address is specified with the **tftp client source** or **tftp** command, this source address is adopted.
- If you use the **tftp client source** command and the **tftp** command to specify a source address respectively, the source address configured with the **tftp** command is used to communicate with a TFTP server.

The source address specified with the **tftp client source** command is valid for all TFTP connections and the source address specified with the **tftp** command is valid only for the current **tftp** connection.

Follow these steps to configure the TFTP client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Use an ACL to control the device's access to TFTP servers | **tftp-server** [ **ipv6** ] **acl** *acl-number* | Optional<br>By default, no ACL is used to control the device's access to TFTP servers. |
| Configure the source address of the TFTP client | **tftp client source** { **interface** *interface-type interface-number* \| **ip** *source-ip-address* } | Optional<br>A device uses the source address determined by the matched route to communicate with the TFTP server by default. |
| Return to user view | **quit** | — |
| Download or upload a file in an IPv4 network | **tftp** *server-address* { **get** \| **put** \| **sget** } *source-filename* [ *destination-filename* ] [ **source** { **interface** *interface-type interface-number* \| **ip** *source-ip-address* } ] | Optional<br>Available in user view |
| Download or upload a file in an IPv6 network | **tftp ipv6** *tftp-ipv6-server* [ **-i** *interface-type interface-number* ] { **get** \| **put** } *source-file* [ *destination-file* ] | Optional<br>Available in user view |

**Note**

- If no primary IP address is configured on the source interface, no TFTP connection can be established.
- If you use the **ftp client source** command to first configure the source interface and then the source IP address of the packets of the TFTP client, the new source IP address will overwrite the current one, and vice versa.

# Displaying and Maintaining the TFTP Client

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the configuration of the TFTP client | **display tftp client configuration** | Available in any view |

# TFTP Client Configuration Example

## Network requirements

- As shown in Figure 3-2, use a PC as the TFTP server and Device as the TFTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. An available route exists between Device and PC.

- Device downloads a startup file from PC for upgrading and uploads a configuration file named **config.cfg** to PC for backup.

**Figure 3-2** Smooth upgrading using the TFTP client function


## Configuration procedure

1) Configure PC (TFTP Server), the configuration procedure is omitted.
- On the PC, enable the TFTP server
- Configure a TFTP working directory

2) Configure Device (TFTP Client)

---

**Caution**

If the available memory space of the device is not enough, use the **fixdisk** command to clear the memory or use the **delete /unreserved** *file-url* command to delete the files not in use and then perform the following operations.

---

# Enter system view.

```
<Sysname> system-view
```

# Download application file **newest.bin** from PC.

```
<Sysname> tftp 1.2.1.1 get newest.bin
```

# Upload a configuration file **config.cfg** to the TFTP server.

```
<Sysname> tftp 1.2.1.1 put config.cfg configback.cfg
```

# Specify **newest.bin** as the main startup file to be used at the next startup.

```
<Sysname> boot-loader file newest.app bbb.bin main
```

# Reboot the device and the software is upgraded.

```
<Sysname> reboot
```

---

**Caution**

The startup file used for the next startup must be saved under the root directory of the storage medium. You can copy or move a file to the root directory of the storage medium. For the details of the **boot-loader** command, refer to *Device Management Commands* in the *System Volume*.

---

# Table of Contents

# 1 HTTP Configuration

When configuring HTTP, go to these sections for information you are interested in:



## HTTP Overview

The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-level protocol in the TCP/IP protocol suite. The connection-oriented Transport Control Protocol (TCP) is adopted on the transport layer.

Currently, HTTP/1.0 is supported on the device.

### How HTTP Works

In the HTTP, the client/server mode is used for communication. The client and the server exchange messages following these procedures:

1) A TCP connection is created between the client and the server. Typically, the port number is 80.
2) The client sends a request to the server.
3) The server processes the request and sends back a response.
4) The TCP connection is closed.

### Logging In to the Device Through HTTP

You can log onto the device using the HTTP protocol with HTTP service enabled, accessing and controlling the device with Web-based network management.

To implement security management on the device, you can use the following methods to enhance the security of the device.

- Enable HTTP service only when necessary.
- Change the port number of the HTTP service as a port number not commonly used (80 or 8080), thus reducing attacks from illegal users on the HTTP service.
- Associate the HTTP service with an ACL to let pass only the filtered clients.

### Protocols and Standards

RFC 1945: Hypertext Transfer Protocol – HTTP/1.0

## Enabling the HTTP Service

The device can act as the HTTP server and the users can access and control the device through the Web function only after the HTTP service is enabled.

Follow these steps to enable the HTTP service:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the HTTP service | **ip http enable** | Required |

## Configuring the Port Number of the HTTP Service

Configuration of the port number of the HTTP service can reduce the attacks from illegal users on the HTTP service.

Follow these steps to configure the port number of the HTTP service:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the port number of the HTTP service | **ip http port** *port-number* | Required<br>By default, the port number of the HTTP service is 80. |

**Note**

If you execute the **ip http port** command for multiple times, the last configured port number is used.

## Associating the HTTP Service with an ACL

By associating the HTTP service with an ACL, only the clients that pass ACL filtering are allowed to access the device.

Follow these steps to associate the HTTP service with an ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enters system view | **system-view** | — |
| Associate the HTTP service with an ACL | **ip http acl** *acl-number* | Required<br>The HTTP service is not associated with an ACL by default. |

## Displaying and Maintaining HTTP

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about HTTP | **display ip http** | Available in any view |

# 2 HTTPS Configuration

When configuring HTTPS, go to these sections for information you are interested in:



## HTTPS Overview

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol.

The SSL protocol of HTTPS enhances the security of the device in the following ways:

- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;
- Encrypts the data exchanged between the HTTPS client and the device to ensure the data security and integrity, thus realizing the security management of the device;
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.

**Note**

- The total number of HTTP connections and HTTPS connections on a device cannot exceed ten.
- For SSL details, refer to *SSL Configuration* in the *Security Volume*.

## HTTPS Configuration Task List

Complete these tasks to configure HTTPS:

| Configuration task | Remarks |
|---|---|
| Associating the HTTPS Service with an SSL Server Policy | Required |
| Enabling the HTTPS Service | Required |
| Associating the HTTPS Service with a Certificate Attribute Access Control Policy | Optional |

| Configuration task | Remarks |
|---|---|
| Configuring the Port Number of the HTTPS Service | Optional |
| Associating the HTTPS Service with an ACL | Optional |

## Associating the HTTPS Service with an SSL Server Policy

You need to associate the HTTPS service with a created SSL server policy before enabling the HTTPS service.

Follow these steps to associate the HTTPS service with an SSL server policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Associate the HTTPS service with an SSL server policy | **ip https ssl-server-policy** *policy-name* | Required<br>Not associated by default |

**Note**

- If the **ip https ssl-server-policy** command is executed repeatedly, the HTTPS service is only associated with the last specified SSL server policy.
- When the HTTPS service is disabled, the association between the HTTPS service and the SSL server is automatically removed. To enable it again, you need to re-associate the HTTPS service with an SSL server policy.
- When the HTTPS service is enabled, no modification of its associated SSL server policy takes effect.

## Enabling the HTTPS Service

The device can act as the HTTPS server and users can access and control the device through the Web function only when the HTTPS service is enabled.

Follow these steps to enable the HTTPS service:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the HTTPS service | **ip https enable** | Required<br>Disabled by default. |

**Note**

- After the HTTPS service is enabled, you can use the **display ip https** command to view the state of the HTTPS service and verify the configuration.
- Enabling of the HTTPS service will trigger an SSL handshake negotiation process. During the process, if the local certificate of the device already exists, the SSL negotiation is successfully performed, and the HTTPS service can be started normally. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Since the application process takes much time, the SSL negotiation may fail and the HTTPS service cannot be started normally. Therefore, the **ip https enable** command must be executed for multiple times to ensure normal startup of the HTTPS service.

## Associating the HTTPS Service with a Certificate Attribute Access Control Policy

Associating the HTTPS service with a configured certificate access control policy helps control the access right of the client, thus providing the device with enhanced security.

Follow these steps to associate the HTTPS service with a certificate attribute access control policy:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Associate the HTTPS service with a certificate attribute access control policy | **ip https certificate access-control-policy** *policy-name* | Required<br>Not associated by default. |

**Note**

- If the **ip https certificate access-control-policy** command is executed repeatedly, the HTTPS server is only associated with the last specified certificate attribute access control policy.
- If the HTTPS service is associated with a certificate attribute access control policy, the **client-verify enable** command must be configured in the SSL server policy. Otherwise, the client cannot log onto the device.
- If the HTTPS service is associated with a certificate attribute access control policy, the latter must contain at least one **permit** rule. Otherwise, no HTTPS client can log onto the device.
- For the configuration of an SSL server policy, refer to *PKI Configuration* in the *Security Volume*.

## Configuring the Port Number of the HTTPS Service

Configuration of the port number of the HTTPS service can reduce the attacks from illegal users on the HTTPS service.

Follow these steps to configure the port number of the HTTPS service:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the port number of the HTTPS service | **ip https port** *port-number* | Optional<br>By default, the port number of the HTTPS service is 443. |

**Note**

If you execute the **ip https port** command for multiple times, the last configured port number is used.

## Associating the HTTPS Service with an ACL

Associating the HTTPS service with an ACL can filter out requests from some clients to let pass only clients that pass the ACL filtering.

Follow these steps to associate the HTTPS service with an ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Associate the HTTPS service with an ACL | **ip https acl** *acl-number* | Required<br>Not associated by default. |

## Displaying and Maintaining HTTPS

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about HTTPS | **display ip https** | Available in any view |

## HTTPS Configuration Example

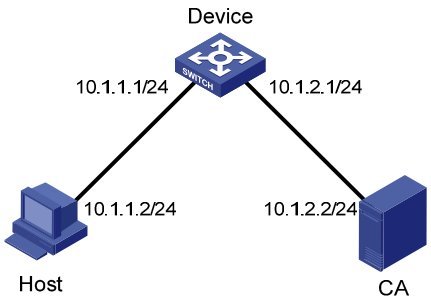
### Network requirements

- Host acts as the HTTPS client and Device acts as the HTTPS server.
- Host accesses Device through Web to control Device.
- CA (Certificate Authority) issues certificate to Device. The common name of CA is **new-ca**.

**Caution**

In this configuration example, Windows Server serves as CA and you need to install Simple Certificate Enrollment Protocol (SCEP) component.

**Figure 2-1** Network diagram for HTTPS configuration




## Configuration procedure

Perform the following configurations on Device:

1) Apply for a certificate for Device

# Configure a PKI entity.

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Configure a PKI domain.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier new-ca
[Device-pki-domain-1] certificate request url http://10.1.2.2:8080/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

# Generate a local RSA key pair.

```
[Device] public-key local create rsa
```

# Obtain a server certificate from CA.

```
[Device] pki retrieval-certificate ca domain 1
```

# Apply for a local certificate.

```
[Device] pki request-certificate domain 1
```

2) Configure an SSL server policy associated with the HTTPS service

# Configure an SSL server policy.

```
[Device] ssl server-policy myssl
[Device-ssl-server-policy-myssl] pki-domain 1
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

3) Configure a certificate access control policy

# Configure a certificate attribute group.

```
[Device] pki certificate attribute-group mygroup1
[Device-pki-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
[Device-pki-cert-attribute-group-mygroup1] quit
```

# Configure certificate access control policy **myacp** and create a control rule.

```
[Device] pki certificate access-control-policy myacp
[Device-pki-cert-acp-myacp] rule 1 permit mygroup1
[Device-pki-cert-acp-myacp] quit
```

4) Reference an SSL server policy

# Associate the HTTPS service with the SSL server policy **myssl**.

```
[Device] ip https ssl-server-policy myssl
```

5) Associate the HTTPS service with a certificate attribute access control policy

# Associate the HTTPS service with certificate attribute access control policy **myacp**.

```
[Device] ip https certificate access-control-policy myacp
```

6) Enable the HTTPS service

# Enable the HTTPS service.

```
[Device] ip https enable
```

7) Verify the configuration

Launch the IE explorer on Host, and enter https://10.1.1.1. You can log in to Device and control it.

---

**Note**

- The URL of the HTTPS server starts with https://, and that of the HTTP server starts with http://.
- For details of PKI commands, refer to *PKI Commands* in the *Security Volume*.
- For details of the **public-key local create rsa** command, refer to *Public Key Commands* in the *Security Volume*.
- For details of SSL commands, refer to *SSL Commands* in the *Security Volume*.

---

# Table of Contents

# 1 SNMP Configuration

When configuring SNMP, go to these sections for information you are interested in:



## SNMP Overview

Simple Network Management Protocol (SNMP) offers a framework to monitor network devices through TCP/IP protocol suite. It provides a set of basic operations in monitoring and maintaining the Internet and has the following characteristics:

- Automatic network management: SNMP enables network administrators to search and modify information, find and diagnose network problems, plan for network growth, and generate reports on network nodes.
- SNMP shields the physical differences between various devices and thus realizes automatic management of products from different manufacturers. Offering only the basic set of functions, SNMP makes the management tasks independent of both the physical features of the managed devices and the underlying networking technology. Thus, SNMP achieves effective management of devices from different manufacturers, especially in small, high-speed and low cost network environments.

### SNMP Mechanism

An SNMP enabled network comprises a Network Management Station (NMS) and an agent.

- An NMS is a station that runs the SNMP client software. It offers a user friendly interface, making it easier for network administrators to perform most network management tasks.
- An agent is a program on the device. It receives and handles requests sent from the NMS. Only under certain circumstances, such as interface state change, will the agent inform the NMS.

An NMS manages an SNMP enabled network, whereas agents are the managed network device. They exchange management information through the SNMP protocol.

SNMP provides the following four basic operations:

- Get operation: The NMS gets the value of one or more objects of the agent through this operation.
- Set operation: The NMS can reconfigure the value of one or more objects in the agent MIB (Management Information Base) by means of this operation.
- Trap operation: The agent sends traps to the NMS through this operation.
- Inform operation: The NMS sends traps to other NMSs through this operation.

## SNMP Protocol Version

Currently, SNMP agents support SNMPv3 and are compatible with SNMPv1 and SNMPv2c.

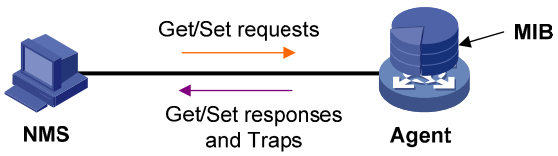
- SNMPv1 uses community name for authentication, which defines the relationship between an SNMP NMS and an SNMP agent. SNMP packets with community names that did not pass the authentication on the device will simply be discarded. A community name performs a similar role as a key word and can be used to regulate access from NMS to agent.
- SNMPv2c uses community name for authentication. Compatible with SNMPv1, it extends the functions of SNMPv1. SNMPv2c provides more operation modes such as GetBulk and InformRequest; it supports more data types such as Counter64; and it provides various error codes, thus being able to distinguish errors in more detail.
- SNMPv3 offers an authentication that is implemented with a User-Based Security Model (USM). You can set the authentication and privacy functions. The former is used to authenticate the validity of the sending end of the authentication packets, preventing access of illegal users; the latter is used to encrypt packets between the NMS and agent, preventing the packets from being intercepted. USM ensures a more secure communication between SNMP NMS and SNMP agent by authentication with privacy, authentication without privacy, or no authentication no privacy.

Successful interaction between NMS and agent requires consistency of SNMP versions configured on them. You can configure multiple SNMP versions for an agent to interact with different NMSs.

## MIB Overview

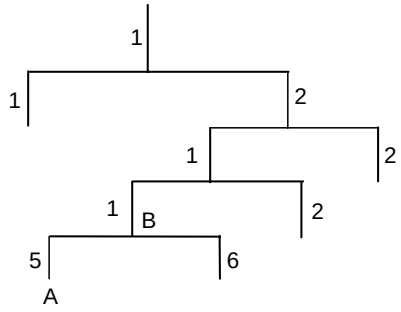
Any managed resource can be identified as an object, which is known as the managed object. Management Information Base (MIB) is a collection of all the managed objects. It defines a set of characteristics associated with the managed objects, such as the object identifier (OID), access right and data type of the objects. Each agent has its own MIB. NMS can read or write the managed objects in the MIB. The relationship between an NMS, agent and MIB is shown in Figure 1-1.

**Figure 1-1** Relationship between NMS, agent and MIB




MIB stores data using a tree structure. The node of the tree is the managed object and can be uniquely identified by a path starting from the root node. As illustrated in the following figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. This string of numbers is the OID of the managed object B.

**Figure 1-2** MIB tree




# SNMP Configuration

As configurations for SNMPv3 differ substantially from those of SNMPv1 and SNMPv2c, their SNMP functionalities is introduced separately below.

Follow these steps to configure SNMPv3:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable SNMP agent | **snmp-agent** | Optional<br>Disabled by default<br>You can enable SNMP agent through this command or any commands that begin with **snmp-agent**. |
| Configure SNMP agent system information | **snmp-agent sys-info** { **contact** *sys-contact* \| **location** *sys-location* \| **version** { **all** \| { **v1** \| **v2c** \| **v3** }***** } } | Optional<br>The defaults are as follows:<br>3Com Corporation. for contact,<br>Marlborough, MA 01752 USA for location, and SNMP v3 for the version. |
| Configure an SNMP agent group | **snmp-agent group v3** *group-name* [ **authentication** \| **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | Required |
| Convert the user-defined plain text password to a cipher text password | **snmp-agent calculate-password** *plain-password* **mode** { **md5** \| **sha \| 3desmd5 \| 3dessha** } { **local-engineid** \| **specified-engineid** *engineid* } | Optional |
| Add a new user to an SNMP agent group | **snmp-agent usm-user v3** *user-name group-name* [ [ **cipher** ] **authentication-mode** { **md5** \| **sha** } *auth-password* [ **privacy-mode** { **3des** \| **aes128** \| **des56** } *priv-password* ] ] [ **acl** *acl-number* ] | Required<br>If the **cipher** keyword is specified, the arguments *auth-password* and *priv-password* are considered as cipher text password. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the maximum size of an SNMP packet that can be received or sent by an SNMP agent | **snmp-agent packet max-size** *byte-count* | Optional<br>1,500 bytes by default |
| Configure the engine ID for a local SNMP agent | **snmp-agent local-engineid** *engineid* | Optional<br>Company ID and device ID by default |
| Create or update the MIB view content for an SNMP agent | **snmp-agent mib-view** { **excluded** \| **included** } *view-name oid-tree* [ **mask** *mask-value* ] | Optional<br>MIB view name is ViewDefault and OID is 1 by default. |

Follow these steps to configure SNMPv1 and SNMPv2c:

| To do… | | | Use the command… | Remarks |
|---|---|---|---|---|
| Enter system view | | | **system-view** | — |
| Enable SNMP agent | | | **snmp-agent** | Optional<br>Disabled by default<br>You can enable SNMP agent through this command or any commands that begin with **snmp-agent**. |
| Configure SNMP agent system information | | | **snmp-agent sys-info** { **contact** *sys-contact* \| **location** *sys-location* \| **version** { { **v1** \| **v2c** \| **v3** }* \| **all** } } | Required<br>The defaults are as follows:<br>3Com Corporation. for contact,<br>Marlborough, MA 01752 USA for location and SNMP v3 for the version. |
| Configure SNMP NMS access right | Configure directly | Create an SNMP community | **snmp-agent community** { **read** \| **write** } *community-name* [ **acl** *acl-number* \| **mib-view** *view-name* ]* | Use either approach.<br>Both commands can be used to configure SNMP NMS access rights. The second command was introduced to be compatible with SNMPv3.<br>The community name configured on NMS should be consistent with the username configured on the agent. |
| | Configure indirectly | Configure an SNMP group | **snmp-agent group** { **v1** \| **v2c** } *group-name* [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | |
| | | Add a new user to an SNMP group | **snmp-agent usm-user** { **v1** \| **v2c** } *user-name group-name* [ **acl** *acl-number* ] | |
| Configure the maximum size of an SNMP packet that can be received or sent by an SNMP agent | | | **snmp-agent packet max-size** *byte-count* | Optional<br>1500 bytes by default |
| Configure the engine ID for a local SNMP agent | | | **snmp-agent local-engineid** *engineid* | Optional<br>Company ID and device ID by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create or update MIB view content for an SNMP agent | **snmp-agent mib-view** { **excluded** \| **included** } *view-name oid-tree* [ **mask** *mask-value* ] | Optional<br>ViewDefault by default |

**Caution**

The validity of a USM user depends on the engine ID of the SNMP agent. If the engine ID when the USM user is created is not identical to the current engine ID, the USM user is invalid.

# Configuring SNMP Logging

## Introduction to SNMP Logging

SNMP logs the GET and SET operations that the NMS performs on the SNMP agent. When the GET operation is performed, the agent logs the IP address of the NMS, node name of the GET operation and OID of the node. When the SET operation is performed, the agent logs the IP address of the NMS, node name of the SET operation, OID of the node, the value set and the error code and error index of the SET response. These logs will be sent to the information center, and the level of them is informational, that is, they are taken as the system prompt information. With parameters for the information center set, the output rules for SNMP logs are decided (that is, whether the logs are permitted to output and the output destinations).

SNMP logs GET request, SET request and SET response, but does not log GET response.

## Enabling SNMP Logging

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable SNMP logging | **snmp-agent log** { **all** \| **get-operation** \| **set-operation** } | Required<br>Disabled by default. |
| Configure SNMP log output rules | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>By default, SNMP logs are output to loghost and logfile only. To output SNMP logs to other destinations such as console or monitor terminal, you need to set the output destinations with this command. |

**Note**

- Logs occupy storage space of the device, thus affecting the performance of the device. Therefore, it is recommended to disable SNMP logging.
- The size of SNMP logs cannot exceed that allowed by the information center, and the total length of the node field and value field of each log record cannot exceed 1K bytes; otherwise, the exceeded part will not be output.
- For the detailed description of system information, the information center and the **info-center source** command, refer to *Information Center Configuration* in the *System Volume*.

# SNMP Trap Configuration

## Enabling the Trap Function

The SNMP agent sends traps to the NMS to inform the NMS of critical and important events (such as reboot of a managed device). Two types of traps are available: generic traps and self-defined traps. Generic traps supported on the device include: **authentication**, **coldstart**, **linkdown**, **linkup** and **warmstart**. The others are self-defined traps, which are generated by different modules. As traps that occupy large device memory affect device performance, it is recommended not to enable the trap function for all the modules but for the specific modules as needed.

With the trap function enabled on a module, the traps generated by the module will be sent to the information center. The information center has seven information output destinations. By default, traps of all modules are allowed to be output to the console, monitor terminal (monitor), loghost, and logfile; traps of all modules and with level equal to or higher than warnings are allowed to be output to the trapbuffer and SNMP module (snmpagent); and traps cannot be sent to the logbuffer. You can set parameters for the information center based on the levels of the traps generated by each module, and thus decide the output rules of traps (that is, whether traps are allowed to be output and the output destinations). For the configuration of the information center, refer to *Information Center Configuration* in the *System Volume*.

Follow these steps to enable the trap function:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the trap function globally | **snmp-agent trap enable** [ **configuration** \| **flash** \| **standard** [ **authentication** \| **coldstart** \| **linkdown** \| **linkup** \| **warmstart** ] * \| **system** ] | Optional<br>By default, the trap function is enabled. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the trap function of interface state changes | **enable snmp trap updown** | Optional<br>Enabled by default. |

**Caution**

To enable an interface to send linkUp/linkDown traps when its state changes, you need to enable the trap function of interface state changes on an interface and globally. Use the **enable snmp trap updown** command to enable the trap function on an interface, and use the **snmp-agent trap enable** [ **standard** [ **linkdown** | **linkup** ] * ] command to enable this function globally.

## Configuring Trap Parameters

### Configuration prerequisites

To send traps to the NMS, you need to prepare the following:

- Basic SNMP configurations have been completed. These configurations include version configuration: community name is needed when SNMPv1 and v2c are adopted; username and MIB view are needed if SNMPv3 is adopted.
- A connection has bee established between the device and the NMS, and they can operate each other.

### Configuration procedure

After traps are sent to the SNMP module, the SNMP module saves the traps in the trap queue. You can set the size of the queue and the holding time of the traps in the queue, and you can also send the traps to the specified destination host (usually the NMS).

Follow these steps to configure trap parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure target host attribute for traps | **snmp-agent target-host trap address udp-domain** { *ip-address* \| **ipv6** *ipv6-address* } [ **udp-port** *port-number* ] **params securityname** *security-string* [ **v1** \| **v2c** \| **v3** [ **authentication** \| **privacy** ] ] | Optional<br>To send the traps to the NMS, this command is required, and you must specify *ip-address* as the IP address of the NMS. |
| Configure the source address for traps | **snmp-agent trap source** *interface-type interface-number* | Optional |
| Extend the standard linkUp/linkDown traps defined in RFC | **snmp-agent trap if-mib link extended** | Optional<br>Standard linkUp/linkDown traps defined in RFC are used by default. |
| Configure the size of the trap sending queue | **snmp-agent trap queue-size** *size* | Optional<br>100 by default |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the holding time of the traps in the queue | **snmp-agent trap life** *seconds* | Optional<br>120 seconds by default |

**Note**

- An extended linkUp/linkDown trap is the standard linkUp/linkDown trap (defined in RFC) appended with interface description and interface type information. If the extended messages are not supported on the NMS, disable this function to let the device send standard linkUp/linkDown traps.
- If the sending queue of traps is full, the system will automatically delete some oldest traps to receive new traps.
- The system will automatically delete the traps whose lifetime expires.

## Displaying and Maintaining SNMP

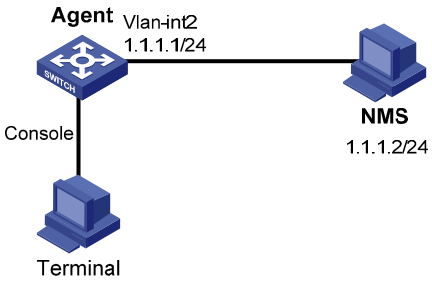
| To do… | Use the command… | Remarks |
|---|---|---|
| Display SNMP-agent system information, including the contact, location, and version of the SNMP | **display snmp-agent sys-info** [ **contact** \| **location** \| **version** ]* | Available in any view |
| Display SNMP agent statistics | **display snmp-agent statistics** | |
| Display the SNMP agent engine ID | **display snmp-agent local-engineid** | |
| Display SNMP agent group information | **display snmp-agent group** [ *group-name* ] | |
| Display basic information of the trap queue | **display snmp-agent trap queue** | |
| Display the modules that can send traps and whether their trap sending is enabled or not | **display snmp-agent trap-list** | |
| Display SNMP v3 agent user information | **display snmp-agent usm-user** [ **engineid** *engineid* \| **username** *user-name* \| **group** *group-name* ] * | |
| Display SNMP v1 or v2c agent community information | **display snmp-agent community** [ **read** \| **write** ] | |
| Display MIB view information for an SNMP agent | **display snmp-agent mib-view** [ **exclude** \| **include** \| **viewname** *view-name* ] | |

# SNMP Configuration Example

## Network requirements

- The NMS connects to the agent, a switch, through an Ethernet.
- The IP address of the NMS is 1.1.1.2/24.
- The IP address of the VLAN interface on the switch is 1.1.1.1/24.
- The NMS monitors and manages the agent using SNMPv2c. The agent reports errors or faults to the NMS.

**Figure 1-3** Network diagram for SNMP




## Configuration procedure

1) Configuring the SNMP agent

# Configure the SNMP basic information, including version and community name.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

# Configure VLAN-interface 2 (with the IP address of 1.1.1.1/24). Add the port GigabitEthernet 1/0/1 to VLAN 2.

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-Vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

# Configure the contact person and physical location information of the switch.

```
[Sysname] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Sysname] snmp-agent sys-info location telephone-closet,3rd-floor
```

# Enable the sending of traps to the NMS with an IP address of 1.1.1.2/24, using **public** as the community name.

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname public
```

2) Configuring the SNMP NMS

With SNMPv2c, the user needs to specify the read only community, the read and write community, the timeout time, and number of retries. The user can inquire and configure the device through the NMS.

**Note**

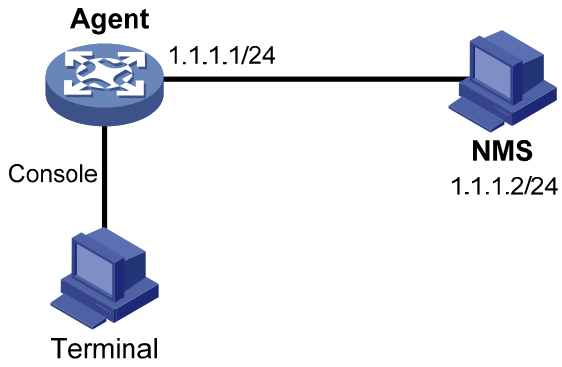
The configurations on the agent and the NMS must match.

# SNMP Logging Configuration Example

## Network requirements

- The NMS and the agent are connected through an Ethernet
- The IP address of the NMS is 1.1.1.2/24
- The IP address of the VLAN interface on the agent is 1.1.1.1/24
- Configure community name, access right and SNMP version on the agent

**Figure 1-4** Network diagram for SNMP logging




## Configuration procedure

**Note**

The configurations for the NMS and agent are omitted.

# Enable logging display on the terminal. (This function is enabled by default, so that you can omit this configuration).

```
<Sysname> terminal monitor
<Sysname> terminal logging
```

# Enable the information center to output the system information with the severity level equal to or higher than **informational** to the console port.

```
<Sysname> system-view
[Sysname] info-center source snmp channel console log level informational
```

# Enable SNMP logging on the agent to log the GET and SET operations of the NMS.

```
[Sysname] snmp-agent log get-operation
[Sysname] snmp-agent log set-operation
```

- The following log information is displayed on the terminal when the NMS performs the GET operation to the agent.

```
%Jan 1 02:49:40:566 2006 Sysname SNMP/6/GET:
seqNO = <10> srcIP = <1.1.1.2> op = <get> node = <sysName(1.3.6.1.2.1.1.5.0)> value=<>
```

- The following log information is displayed on the terminal when the NMS performs the SET operation to the agent.

```
%Jan 1 02:59:42:576 2006 Sysname SNMP/6/SET:
seqNO = <11> srcIP = <1.1.1.2> op = <set> errorIndex = <0> errorStatus =<noError> node =
<sysName(1.3.6.1.2.1.1.5.0)> value = <Sysname>
```

**Table 1-1** Description on the output field of SNMP log

| Field | Description |
|---|---|
| Jan 1 02:49:40:566 2006 | The time when SNMP log is generated |
| seqNO | Sequence number of the SNMP log () |
| srcIP | IP address of NMS |
| op | SNMP operation type (GET or SET) |
| node | Node name of the SNMP operations and OID of the instance |
| erroIndex | Error index, with 0 meaning no error |
| errorstatus | Error status, with noError meaning no error |
| value | Value set when the SET operation is performed (This field is null, meaning the value obtained with the GET operation is not logged.)<br>When the value is a string of characters and the string contains characters not in the range of ASCII 0 to 127 or invisible characters, the string is displayed in hexadecimal. For example, value = <81-43>[hex] |

**Note**

The system information of the information center can be output to the terminal or to the log buffer. In this example, SNMP log is output to the terminal. For configuration of SNMP log output to other destinations, see *Information Center Configuration* in the *System Volume*.

# 2 MIB Style Configuration

3Com private MIB involves two styles, 3Com compatible MIB and 3Com new MIB. In the 3Com compatible MIB style, the device sysOID is under the 3Com's enterprise ID 25506, and the private MIB is under the enterprise ID 2011. In the 3Com new MIB style, both the device sysOID and the private MIB are under the 3Com's enterprise ID 25506. These two styles of MIBs implement the same management function except for their root nodes. A device is shipped with MIB loaded and the MIB style may vary depending on the device. To implement NMS's flexible management of the device, the device allows you to configure MIB style, that is, you can switch between the two styles of MIBs. However, you need to ensure that the MIB style of the device is the same as that of the NMS.

## Setting the MIB Style

Follow these steps to set the MIB style:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the MIB style of the device | **mib-style** [ **new** \| **compatible** ] | Optional<br>**new** by default |

**Note**

The modified MIB style takes effect only after you reboot the device. Therefore, you are recommended to reboot the device after setting the MIB style to ensure that the modification of the MIB style takes effect.

## Displaying and Maintaining MIB

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the MIB style | **display mib-style** | Available in any view |

# Table of Contents

# 1 RMON Configuration

When configuring RMON, go to these sections for information you are interested in:



## RMON Overview

This section covers these topics:



### Introduction

Remote Monitoring (RMON) is implemented based on the Simple Network Management Protocol (SNMP) and is fully compatible with the existing SNMP framework without the need of any modification on SNMP.

RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. It reduces traffic between network management station (NMS) and agent, facilitating large network management.

RMON comprises two parts: NMSs and agents running on network devices.

- Each RMON NMS administers the agents within its administrative domain.
- An RMON agent resides on a network monitor or a network probe. It monitors and collects statistics on traffic over the network segments connected to its interfaces, such as the total number of packets passed through a network segment over a specified period, or the total number of good packets sent to a host.

### Working Mechanism

RMON allows multiple monitors. A monitor provides two ways of data gathering:

- Using RMON probes. NMSs can obtain management information from RMON probes directly and control network resources. In this approach, RMON NMSs can obtain all RMON MIB information.
- Embedding RMON agents in network devices such as routers, switches, and hubs to provide the RMON probe function. RMON NMSs exchange data with RMON agents using basic SNMP commands to gather network management information, which, due to system resources limitation, may not cover all MIB information but four groups of information, alarm, event, history, and statistics, in most cases.

The device adopts the second way. By using RMON agents on network monitors, an NMS can obtain information about traffic size, error statistics, and performance statistics for network management.

## RMON Groups

Among the ten RMON groups defined by RMON specifications (RFC 1757), the device supports the event group, alarm group, history group and statistics group. Besides, 3Com also defines and implements the private alarm group, which enhances the functions of the alarm group. This section describes the five kinds of groups in general.

### Event group

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group and the private alarm group. The events can be handled in one of the following ways:

- Logging event related information in the event log table
- Sending traps to NMSs
- Logging event information in the event log table and sending traps to NMSs
- No action

### Alarm group

The RMON alarm group monitors specified alarm variables, such as statistics on a port. If the sampled value of the monitored variable is bigger than or equal to the upper threshold, an upper event is triggered; if the sampled value of the monitored variable is lower than or equal to the lower threshold, a lower event is triggered. The event is then handled as defined in the event group.

The following is how the system handles entries in the RMON alarm table:

1) Samples the alarm variables at the specified interval.
2) Compares the sampled values with the predefined threshold and triggers events if all triggering conditions are met.

---

**Note**

If a sampled alarm variable overpasses the same threshold multiple times, only the first one can cause an alarm event. That is, the rising alarm and falling alarm are alternate.

---

### Private alarm group

The private alarm group calculates the sampled values of alarm variables and compares the result with the defined threshold, thereby realizing a more comprehensive alarming function.

System handles the prialarm alarm table entry (as defined by the user) in the following ways:

- Periodically samples the prialarm alarm variables defined in the prialarm formula.
- Calculates the sampled values based on the prialarm formula.
- Compares the result with the defined threshold and generates an appropriate event.

**Note**

If the count result overpasses the same threshold multiple times, only the first one can cause an alarm event. That is, the rising alarm and falling alarm are alternate.

### History group

The history group periodically collects statistics on data at interfaces and saves the statistics in the history record table for query convenience. The statistics data includes bandwidth utilization, number of error packets, and total number of packets.

Once you successfully create a history entry in the specified interface, the history group starts to periodically collect statistics on packet at the specified interface. Each statistical value is a cumulative sum of packets sent/received on the interface during a sampling period.

### Ethernet statistics group

The statistics group monitors port utilization. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, bytes sent, packets sent, and so on.

After the creation of a statistics entry on an interface, the statistics group starts to collect traffic statistics on the current interface. The result of the statistics is a cumulative sum.

# Configuring RMON

## Configuration Prerequisites

Before configuring RMON, configure the SNMP agent as described in *SNMP Configuration* in the *System Volume*.

## Configuration Procedure

Follow these steps to configure RMON:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an event entry in the event table | **rmon event** *entry-number* [ **description** *string* ] { **log** \| **log-trap** *log-trapcommunity* \| **none** \| **trap** *trap-community* } [ **owner** *text* ] | Optional |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Create an entry in the history table | **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [ **owner** *text* ] | Optional |
| Create an entry in the statistics table | **rmon statistics** *entry-number* [ **owner** *text* ] | Optional |
| Exit Ethernet interface view | **quit** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create an entry in the alarm table | **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** \| **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [ **owner** *text* ] | Optional |
| Create an entry in the private alarm table | **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** \| **changeratio** \| **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** \| **cycle** *cycle-period* } [ **owner** *text* ] | Optional |

**Note**

- A new entry cannot be created if its parameters are identical with the corresponding parameters of an existing entry Refer to Table 1-1 for the parameters to be compared for different entries.
- The system limits the total number of each type of entries (Refer to Table 1-1 for the detailed numbers). When the total number of an entry reaches the maximum number of entries that can be created, the creation fails.
- When you create an entry in the history table, if the specified **buckets** *number* argument exceeds the history table size supported by the device, the entry will be created. However, the validated value of the **buckets** *number* argument corresponding to the entry is the history table size supported by the device.

**Table 1-1** Restrictions on the configuration of RMON

| Entry | Parameters to be compared | Maximum number of entries that can be created |
|---|---|---|
| Event | Event description (**description** *string*), event type (**log**, **trap**, **logtrap** or **none**) and community name (*trap-community* or *log-trapcommunity*) | 60 |
| History | Sampling interval (**interval** *sampling-interval*) | 100 |
| Statistics | Only one statistics entry can be created on an interface. | 100 |
| Alarm | Alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) | 60 |
| Prialarm | Alarm variable formula (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute, changeratio** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) | 50 |

# Displaying and Maintaining RMON

| To do… | Use the command… | Remarks |
|---|---|---|
| Display RMON statistics | **display rmon statistics** [ *interface-type interface-number* ] | Available in any view |
| Display the RMON history control entry and history sampling information | **display rmon history** [ *interface-type interface-number* ] | Available in any view |
| Display RMON alarm configuration information | **display rmon alarm** [ *entry-number* ] | Available in any view |
| Display RMON prialarm configuration information | **display rmon prialarm** [ *entry-number* ] | Available in any view |
| Display RMON events configuration information | **display rmon event** [ *entry-number* ] | Available in any view |
| Display log information for the specified or all event entries. | **display rmon eventlog** [ *entry-number* ] | Available in any view |

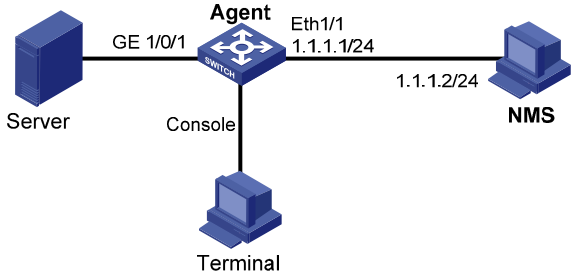
# RMON Configuration Example

## Network requirements

Agent is connected to a configuration terminal through its console port and to a remote NMS across the Internet.

Create an entry in the RMON Ethernet statistics table to gather statistics on GigabitEthernet 1/0/1, and enable logging after received bytes exceed the specified threshold.

**Figure 1-1** Network diagram for RMON




## Configuration procedure

# Configure RMON to gather statistics for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1-rmon
[Sysname-GigabitEthernet1/0/1] quit
```

# Display RMON statistics for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics GigabitEthernet 1/0/1
Statistics entry 1 owned by user1-rmon is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 21657     , etherStatsPkts          : 307
```

```
  etherStatsBroadcastPkts  : 56        , etherStatsMulticastPkts : 34
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 235       ,  65-127  : 67        ,  128-255  : 4
  256-511: 1         ,  512-1023: 0         ,  1024-1518: 0
```

# Create an event to start logging after the event is triggered.

```
<Sysname> system-view
[Sysname] rmon event 1 log owner 1-rmon
```

# Configure an alarm group to sample received bytes on GigabitEthernet 1/0/1. When the received bytes exceed the upper or below the lower limit, logging is enabled.

```
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 delta rising-threshold 1000 1
falling-threshold 100 1 owner 1-rmon
[Sysname] display rmon alarm 1
Alarm table 1 owned by 1-rmon is VALID.
  Samples type          : delta
  Variable formula      : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval     : 10(sec)
  Rising threshold      : 1000(linked with event 1)
  Falling threshold     : 100(linked with event 1)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 2552
```

# Table of Contents

# 1 MAC Address Table Management Configuration

When configuring MAC address table management, go to these sections for information you are interested in:



**Note**

- Interfaces that MAC address table management involves can only be Layer 2 Ethernet ports.
- This manual covers only the management of static, dynamic and blackhole MAC address table entries (source and destination). For the management of multicast MAC address table entries, refer to *Multicast Routing and Forwarding Configuration* in the *IP Multicast Volume*.

## Introduction to MAC Address Table

A device maintains a MAC address table for frame forwarding. Each entry in this table indicates the MAC address of a connected device, ID of the interface to which this device is connected and ID of the VLAN to which the interface belongs. When forwarding a frame, the device looks up the MAC address table according to the destination MAC address of the frame to rapidly determine the egress port, thus reducing broadcasts.

### How a MAC Address Table Entry is Generated

A MAC address table entry can be dynamically learned or manually configured.

#### Dynamically learn a MAC address table entry

Usually, MAC address tables are automatically generated during the source MAC address learning process of devices.

The following is how a device learns a MAC address after it receives a frame from a port, Port 1 for example:

1) Check the source MAC address (MAC-SOURCE for example) of the frame, that is, the MAC address of the device that sends the frame.
2) Look up the MAC address table for an entry corresponding to the MAC address and do the following:

- If an entry is found for the MAC address, update the entry.
- If no entry is found, add an entry for the MAC address to indicate from which port the frame is received.

When receiving a frame destined for MAC-SOURCE, the device then looks up the MAC address table and forwards it from Port 1.

To adapt to network changes, MAC address table entries need to be constantly updated. Each dynamically learned MAC address table entry has a life period, that is, an aging timer. If an entry is not updated before the aging timer expires, it will be deleted. If yes, the aging timer restarts the timing.

### Manually configure a MAC address table entry

When a device dynamically learns MAC address table entries through source MAC address learning, it cannot tell frames of legal users from those of hackers. This brings potential security hazards. For example, if a hacker forges the MAC address of a legal user and uses it as the source MAC address of the attack frames, and accesses the device from a different port than that used by the legal user, the device will learn a forged MAC address entry, and forward frames destined for the legal user to the hacker instead.

To enhance the security of a port, you can manually add MAC address entries into the MAC address table of the device to bind specific user devices to the port, thus preventing hackers from stealing data using forged MAC addresses. Manually configured MAC address table entries have a higher priority than dynamically learned ones.

## Types of MAC Address Table Entries

A MAC address table may contain the following types of entries:

- Static entries, which are manually configured and never age out.
- Dynamic entries, which can be manually configured or dynamically learned and may age out.
- Blackhole entries, which are manually configured and never age out. Blackhole entries are configured to filter frames with specific source or destination MAC addresses.

---

**Note**

Dynamically-learned MAC addresses cannot overwrite static or blackhole MAC address entries, but the latter can overwrite the former.

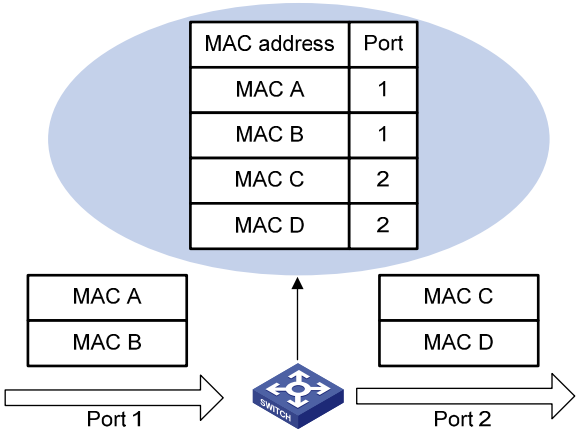
---

## MAC Address Table-Based Frame Forwarding

When forwarding a frame, the device adopts the following two forwarding modes based on the MAC address table:

- Unicast mode: If an entry is available for the destination MAC address, the device forwards the frame out the outgoing interface indicated by the MAC address table entry.
- Broadcast mode: If the device receives a frame with the destination address being all ones, or no entry is available for the destination MAC address, the device broadcasts the frame to all the interfaces except the receiving interface.

**Figure 1-1** Forward frames using the MAC address table




# Configuring MAC Address Table Management

The MAC address table management configuration tasks include:

- Configuring MAC Address Table Entries
- Configuring the Aging Timer for Dynamic MAC Address Entries
- Configuring the MAC Learning Limit

These configuration tasks are all optional and randomly sorted. You can choose some of the configuration tasks as required.

## Configuring MAC Address Table Entries

Follow these steps to add, modify, or remove entries in the MAC address table globally:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Add/modify a MAC address entry | **mac-address blackhole** *mac-address* **vlan** *vlan-id* | Required |
| | **mac-address** { **dynamic** \| **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* | |

Follow these steps to add, modify, or remove entries in the MAC address table on an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Add/modify MAC address entries under the specified interface view | **mac-address** { **dynamic** \| **static** } *mac-address* **vlan** *vlan-id* | Required |

## Configuring the Aging Timer for Dynamic MAC Address Entries

The MAC address table on your device is available with an aging mechanism for dynamic entries to prevent its resources from being exhausted. Set the aging timer appropriately: a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate the latest network changes; a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance.

Follow these steps to configure the aging timer for dynamic MAC address entries:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the aging timer for dynamic MAC address entries | **mac-address timer** { **aging** *seconds* \| **no-aging** } | Optional<br>300 by default. |

**Note**

The aging timer for dynamic MAC address entries takes effect globally on dynamic MAC address entries (learned or administratively configured) only.

## Configuring the MAC Learning Limit

To prevent a MAC address table from getting so large that it may degrade forwarding performance, you may restrict the number of MAC addresses that can be learned on a per-port, port group basis.

Follow these steps to configure the MAC learning limit:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter Ethernet interface view, port group view, or Layer 2 aggregate interface view | Enter Ethernet interface view | **interface** *interface-type interface-number* | Required<br>Use any of these three commands.<br>The configuration you make in Ethernet interface view or Layer 2 aggregate interface view takes effect on the current interface only; the configuration you make in port group view takes effect on all the member ports in the port group. |
| | Enter port group view | **port-group manual** *port-group-name* | |
| | Enter Layer 2 aggregate interface view | **interface bridge-aggregation** *interface-number* | |
| Configure the maximum number of MAC addresses that can be learned on an Ethernet port view or port group | | **mac-address max-mac-count** *count* | Required<br>The default maximum number of MAC addresses that can be learned is not configured. |

# Displaying and Maintaining MAC Address Table Management

| To do… | Use the command… | Remarks |
|---|---|---|
| Display MAC address table information | **display mac-address blackhole** [ **vlan** *vlan-id* ] [ **count** ] | Available in any view |
| | **display mac-address** [ *mac-address* [ **vlan** *vlan-id* ] \| [ **dynamic** \| **static** ] [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] [ **count** ] ] | |
| Display the aging timer for dynamic MAC address entries | **display mac-address aging-time** | |
| Display MAC address statistics | **display mac-address statistics** | |

# MAC Address Table Management Configuration Example

## Network requirements

Log onto your device from the Console port to configure MAC address table management as follows:

- Set the aging timer to 500 seconds for dynamic MAC address entries.
- Add a static entry 000f-e235-dc71 for port GigabitEthernet 1/0/1 in VLAN 1.

## Configuration procedure

# Add a static MAC address entry.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

# Set the aging timer for dynamic MAC address entries to 500 seconds.

```
[Sysname] mac-address timer aging 500
```

# Display the MAC address entry for port GigabitEthernet 1/0/1.

```
[Sysname] display mac-address interface gigabitethernet 1/0/1
MAC ADDR          VLAN ID  STATE           PORT INDEX              AGING TIME(s)

000f-e235-dc71    1        Config static   GigabitEthernet 1/0/1   NOAGED

  ---  1 mac address(es) found  ---
```

# 2 MAC Information Configuration

When configuring MAC Information, go to these sections for information you are interested in:



## Overview

### Introduction to MAC Information

To monitor a network, you need to monitor users joining and leaving the network. Because a MAC address uniquely identifies a network user, you can monitor users joining and leaving a network by monitoring their MAC addresses.

With the MAC Information function, Layer-2 Ethernet interfaces send Syslog or Trap messages to the monitor end in the network when they learn or delete MAC addresses. By analyzing these messages, the monitor end can monitor users accessing the network.

### How MAC Information Works

When a new MAC address is learned or an existing MAC address is deleted on a device, the device writes related information about the MAC address to the buffer area used to store user information. When the timer set for sending MAC address monitoring Syslog or Trap messages expires, or when the buffer is used up, the device sends the Syslog or Trap messages to the monitor end immediately.

## Configuring MAC Information

The MAC Information configuration tasks include:



### Enabling MAC Information Globally

Follow these steps to enable MAC Information globally:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable MAC Information globally | **mac-address information enable** | Required<br>Disabled by default |

## Enabling MAC Information on an Interface

Follow these steps to enable MAC Information on an interface:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable MAC Information on the interface | **mac-address information enable** { **added** \| **deleted** } | Required<br>Disabled by default |

**Note**

To enable MAC Information on an Ethernet interface, enable MAC Information globally first.

## Configuring MAC Information Mode

Follow these steps to configure MAC Information mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure MAC Information mode | **mac-address information mode** { **syslog** \| **trap** } | Optional<br>**trap** by default |

## Configuring the Interval for Sending Syslog or Trap Messages

To prevent Syslog or Trap messages being sent too frequently and thus affecting system performance, you can set the interval for sending Syslog or Trap messages.

Follow these steps to set the interval for sending Syslog or Trap messages:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the interval for sending Syslog or Trap messages | **mac-address information interval** *interval-time* | Optional<br>One second by default. |

## Configuring the MAC Information Queue Length

To avoid losing user MAC address information, when the buffer storing user MAC address information is used up, the user MAC address information in the buffer is sent to the monitor end in the network, even if the timer set for sending MAC address monitoring Syslog or Trap messages has not expired yet.

Follow these steps to configure the MAC Information queue length:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the MAC Information queue length | **mac-address information queue-length** *value* | Optional<br>50 by default |

**Note**

Setting the MAC Information queue length to 0 indicates that the device sends a Syslog or Trap message to the network management device as soon as a new MAC address is learned or an existing MAC address is deleted.

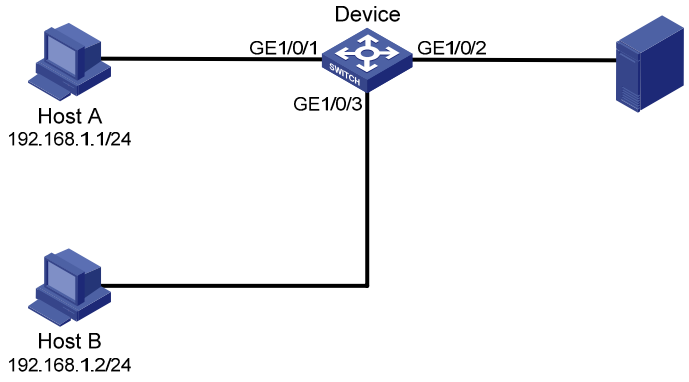
# MAC Information Configuration Example

## MAC Information Configuration Example

### Network requirements

- Host A is connected to a remote server (Server) through Device.
- Enable MAC Information on GigabitEthernet 1/0/1 on Device. Device sends MAC address change information using Syslog messages to Host B through GigabitEthernet 1/0/3. Host B analyzes and displays the Syslog messages.

**Figure 2-1** Network diagram for MAC Information configuration




### Configuration procedure

1) Configure Device to send Syslog messages to Host B.

Refer to *Information Center Configuration* in the *System Volume* for details.

2) Enable MAC Information.

# Enable MAC Information on Device.

```
<Device> system-view
[Device] mac-address information enable
```

# Configure MAC Information mode as Syslog.

```
[Device] mac-address information mode syslog
```

# Enable MAC Information on GigabitEthernet 1/0/1

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-address information enable added
[Device-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-GigabitEthernet1/0/1] quit
```

# Set the MAC Information queue length to 100.

```
[Device] mac-address information queue-length 100
```

# Set the interval for sending Syslog or Trap messages to 20 seconds.

```
[Device] mac-address information interval 20
```

# Table of Contents

# 1 System Maintaining and Debugging

When maintaining and debugging the system, go to these sections for information you are interested in:



## System Maintaining and Debugging Overview

### Introduction to System Maintaining

You can use the **ping** command and the **tracert** command to verify the current network connectivity.

#### The ping command

You can use the **ping** command to verify whether a device with a specified address is reachable, and to examine network connectivity.

The **ping** command involves the following steps in its execution:

1) The source device sends an ICMP echo request to the destination device.
2) If the network is functioning properly, the destination device responds by sending an ICMP echo reply to the source device after receiving the ICMP echo request.
3) If there is network failure, the source device displays timeout or destination unreachable.
4) The source device displays related statistics.

Output of the **ping** command falls into the following:

- The **ping** command can be applied to the destination's name or IP address. If the destination's name is unknown, the prompt information is displayed.
- Information on the destination's responses towards each ICMP echo request. If the source device does not receive an ICMP echo reply within the timeout time, it displays the prompt information. If the source device receives an ICMP echo reply within the timeout time, it displays the number of bytes of the echo reply, the message sequence number, Time to Live (TTL), the response time, and the statistics during the ping operation. The statistics include number of packets sent, number of echo reply messages received, percentage of packets not responded to the total packets sent, and the minimum, average, and maximum response time.

#### The tracert command

By using the **tracert** command, you can trace the Layer 3 devices involved in delivering a packet from source to destination. This is useful for identification of failed node(s) in the event of network failure.

The **tracert** command involves the following steps in its execution:

1) The source device sends a packet with a TTL value of 1 to the destination device.

2) The first hop (the Layer 3 device that first receives the packet) responds by sending a TTL-expired ICMP message to the source, with its IP address encapsulated. In this way, the source device can get the address of the first Layer 3 device.
3) The source device sends a packet with a TTL value of 2 to the destination device.
4) The second hop responds with a TTL-expired ICMP message, which gives the source device the address of the second Layer 3 device.
5) The above process continues until the ultimate destination device is reached. In this way, the source device can trace the addresses of all the Layer 3 devices involved to get to the destination device.

## Introduction to System Debugging

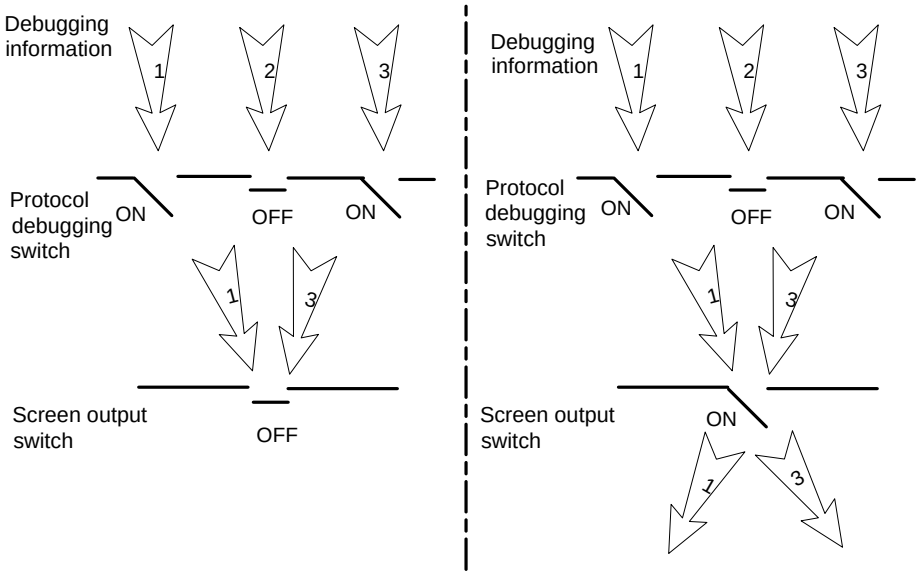
The device provides various debugging functions. For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors.

The following two switches control the display of debugging information:

- Protocol debugging switch, which controls protocol-specific debugging information.
- Screen output switch, which controls whether to display the debugging information on a certain screen.

As Figure 1-1 illustrates, suppose the device can provide debugging for the three modules 1, 2, and 3. Only when both the protocol debugging switch and the screen output switch are turned on can debugging information be output on a terminal.

**Figure 1-1** The relationship between the protocol and screen debugging switch




**Note**

Outputting debugging information to a terminal is most commonly used. You can also configure to output debugging information to other directions. For detailed configuration, refer to *Information Center Configuration* in the *System Volume*.

# System Maintaining and Debugging

## System Maintaining

| To do… | Use the command… | Remarks |
|---|---|---|
| Check whether a specified IP address can be reached | **ping** [ **ip** ] [ **-a** *source-ip* \| **-c** *count* \| **-f** \| **-h** *ttl* \| **-i** *interface-type interface-number* \| **-m** *interval* \| **-n** \| **-p** *pad* \| **-q** \| **-r** \| **-s** *packet-size* \| **-t** *timeout* \| **-tos** *tos* \| **-v** ] * *remote-system* | Optional<br>Used in IPv4 network<br>Available in any view |
| | **ping ipv6** [ **-a** *source-ipv6* \| **-c** *count* \| **-m** *interval* \| **-s** *packet-size* \| **-t** *timeout* ] * *remote-system* [ **-i** *interface-type interface-number* ] | Optional<br>Used in IPv6 network<br>Available in any view |
| View the route from the source to the destination | **tracert** [ **-a** *source-ip* \| **-f** *first-ttl* \| **-m** *max-ttl* \| **-p** *port* \| **-q** *packet-number* \| **-w** *timeout* ] * *remote-system* | Optional<br>Used in IPv4 network<br>Available in any view |
| | **tracert ipv6** [ **-f** *first-ttl* \| **-m** *max-ttl* \| **-p** *port* \| **-q** *packet-number* \| **-w** *timeout* ] * *remote-system* | Optional<br>Used in IPv6 network<br>Available in any view |

**Note**

- For a low-speed network, you are recommended to set a larger value for the timeout timer (indicated by the **-t** parameter in the command) when configuring the **ping** command.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

## System Debugging

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the terminal monitoring of system information | **terminal monitor** | Optional<br>The terminal monitoring on the console is enabled by default and that on the monitoring terminal is disabled by default.<br>Available in user view |
| Enable the terminal display of debugging information | **terminal debugging** | Required<br>Disabled by default<br>Available in user view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable debugging for a specified module | **debugging** { **all** [ **timeout** *time* ] \| *module-name* [ *option* ] } | Required<br>Disabled by default<br>Available in user view |
| Display the enabled debugging functions | **display debugging** [ **interface** *interface-type interface-number* ]<br>[ *module-name* ] | Optional<br>Available in any view |

**Note**

- The **debugging** commands are usually used by administrators in diagnosing network failure.
- Output of the debugging information may reduce system efficiency, especially during execution of the **debugging all** command.
- After completing the debugging, you are recommended to use the **undo debugging all** command to disable all the debugging functions.
- You must configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display the detailed debugging information on the terminal. For the detailed description on the **terminal debugging** and **terminal monitor** commands, refer to *Information Center Commands* in the *System Volume*.

# System Maintaining Example

## Network requirements

- The IP address of the destination device is 10.1.1.4.
- Display the Layer 3 devices involved while packets are forwarded from the source device to the destination device.

## Configuration procedure

```
<Sysname> tracert 10.1.1.4
traceroute to 10.1.1.4 (10.1.1.4) 30 hops max, 40 bytes packet
1  128.3.112.1  19 ms  19 ms  0 ms
2  128.32.216.1  39 ms  39 ms  19 ms
3  128.32.136.23  39 ms  40 ms  39 ms
4  128.32.168.22  39 ms  39 ms  39 ms
5  128.32.197.4  40 ms  59 ms  59 ms
6  131.119.2.5  59 ms  59 ms  59 ms
7  129.140.70.13  99 ms  99 ms  80 ms
8  129.140.71.6  139 ms  239 ms  319 ms
9  129.140.81.7  220 ms  199 ms  199 ms
10  10.1.1.4  239 ms  239 ms  239 ms
```

The above output shows that nine Layer 3 devices are used from the source to the destination device.

# Table of Contents

# 1 Information Center Configuration

When configuring information center, go to these sections for information you are interested in:



## Information Center Overview

### Introduction to Information Center

Acting as the system information hub, information center classifies and manages system information, offering a powerful support for network administrators and developers in monitoring network performance and diagnosing network problems.

The following describes the working process of information center:

- Receives the log, trap, and debugging information generated by each module.
- Outputs the above information to different information channels according to the user-defined output rules.
- Outputs the information to different destinations based on the information channel-to-destination associations.

To sum up, information center assigns the log, trap and debugging information to the ten information channels according to the eight severity levels and then outputs the information to different destinations. The following describes the working process in details.

---

 **Note**

By default, the information center is enabled. An enabled information center affects the system performance in some degree due to information classification and output. Such impact becomes more obvious in the event that there is enormous information waiting for processing.

---

#### Classification of system information

The system information of the information center falls into three types:

- Log information
- Trap information
- Debugging information

### Eight levels of system information

The information is classified into eight levels by severity. The severity levels in the descending order are emergency, alert, critical, error, warning, notice, informational and debug. When the system information is output by level, the information with severity level higher than or equal to the specified level is output. For example, in the output rule, if you configure to output information with severity level being informational, the information with severity level being emergency through informational is all allowed to be output.

**Table 1-1** Severity description

| Severity | Severity value | Description |
|---|---|---|
| Emergency | 0 | The system is unusable. |
| Alert | 1 | Action must be taken immediately |
| Critical | 2 | Critical conditions |
| Error | 3 | Error conditions |
| Warning | 4 | Warning conditions |
| Notice | 5 | Normal but significant condition |
| Informational | 6 | Informational messages |
| Debug | 7 | Debug-level messages |

### Six output destinations and ten channels of system information

The system supports six information output destinations, including the console, monitor terminal (monitor), log buffer, log host, trap buffer and SNMP module. The specific destinations supported vary with devices.

The system supports ten channels. The six channels 0 through 5 are configured with channel names, output rules, and are associated with output destinations by default. The channel names, output rules and the associations between the channels and output destinations can be changed through commands. Besides, you can configure channels 6, 7, 8, and 9 without changing the default configuration of the six channels.

**Table 1-2** Information channels and output destinations

| Information channel number | Default channel name | Default output destination | Note |
|---|---|---|---|
| 0 | console | Console | Receives log, trap and debugging information |
| 1 | monitor | Monitor terminal | Receives log, trap and debugging information, facilitating remote maintenance |
| 2 | loghost | Log host | Receives log, trap and debugging information and information will be stored in files for future retrieval. |
| 3 | trapbuffer | Trap buffer | Receives trap information, a buffer inside the router for recording information. |

| Information channel number | Default channel name | Default output destination | Note |
|---|---|---|---|
| 4 | logbuffer | Log buffer | Receives log and debugging information, a buffer inside the router for recording information. |
| 5 | snmpagent | SNMP module | Receives trap information |
| 6 | channel6 | Not specified | Receives log, trap, and debugging information |
| 7 | channel7 | Not specified | Receives log, trap, and debugging information |
| 8 | channel8 | Not specified | Receives log, trap, and debugging information |
| 9 | channel9 | Log file | Receives log, trap, and debugging information |

**Note**

Configurations for the six output destinations function independently and take effect only after the information center is enabled.

### Outputting system information by source module

The system is composed of a variety of protocol modules, and configuration modules. The system information can be classified, filtered, and output according to source modules. You can use the **info-center source ?** command to view the supported information source modules.

### Default output rules of system information

The default output rules define the source modules allowed to output information on each output destination, the output information type, and the output information level as shown in Table 1-3, which indicates that by default and in terms of all modules:

- Log information with severity level equal to or higher than informational is allowed to be output to the log host; log information with severity level equal to or higher than warning is allowed to be output to the console, monitor terminal, and log buffer; log information is not allowed to be output to the trap buffer and the SNMP module.
- All trap information is allowed to be output to the console, monitor terminal and log host; trap information with severity level equal to or higher than warning is allowed to be output to the trap buffer and SNMP module; trap information is not allowed to be output to the log buffer.
- All debugging information is allowed to be output to the console and monitor terminal; debugging information is not allowed to be output to the log host, log buffer, trap buffer and the SNMP module.

**Table 1-3** Default output rules for different output destinations

| Output destination | Modules allowed | LOG | | TRAP | | DEBUG | |
|---|---|---|---|---|---|---|---|
| | | Enabled/ disabled | Severity | Enabled/ disabled | Severity | Enabled/ disabled | Severity |
| Console | default (all modules) | Enabled | Warning | Enabled | Debug | Enabled | Debug |
| Monitor terminal | default (all modules) | Enabled | Warning | Enabled | Debug | Enabled | Debug |
| Log host | default (all modules) | Enabled | Informational | Enabled | Debug | Disabled | Debug |
| Trap buffer | default (all modules) | Disabled | Informational | Enabled | Warning | Disabled | Debug |
| Log buffer | default (all modules) | Enabled | Warning | Disabled | Debug | Disabled | Debug |
| SNMP module | default (all modules) | Disabled | Debug | Enabled | Warning | Disabled | Debug |

## System Information Format

The format of system information varies with the output destinations.

- If the output destination is not the log host (such as console, monitor terminal, logbuffer, trapbuffer, SNMP), the system information is in the following format:

```
timestamp sysname module/level/digest:content
```

For example, a monitor terminal connects to the device. When a terminal logs in to the device, the log information in the following format is displayed on the monitor terminal:

```
%Jun 26 17:08:35:809 2008 Sysname SHELL/4/LOGIN: VTY login from 1.1.1.1
```

- If the output destination is the log host, the system information is in the following format according to RFC 3164 (The BSD Syslog Protocol):

```
<Int_16>timestamp sysname %%nnmodule/level/digest: source content
```

---

**Note**

- The closing set of angel brackets < >, the space, the forward slash /, and the colon are all required in the above format.
- The format in the previous part is the original format of system information, so you may see the information in a different format. The displayed format depends on the tools you use to view the logs.

---

What follows is a detailed explanation of the fields involved:

### Int_16 (priority)

The priority is calculated using the following formula: facility*8+severity, in which facility represents the logging facility name and can be configured when you set the log host parameters. The facility ranges from local0 to local7 (16 to 23 in decimal integers) and defaults to local7. The facility is mainly used to mark different log sources on the log host, query and filter the logs of the corresponding log source. Severity ranges from 0 to 7. Table 1-1 details the value and meaning associated with each severity.

Note that the priority field takes effect only when the information has been sent to the log host.

### timestamp

Timestamp records the time when system information is generated to allow users to check and identify system events. You can use the **info-center timestamp** command to configure whether to include a timestamp in the system information as well as the timestamp format if it is included. The time stamp of the system information sent from the information center to the log host is with a precision of seconds, whereas that of the system information sent from the information center to the other destinations is with a precision of milliseconds.

### sysname

Sysname is the system name of the current host. You can use the **sysname** command to modify the system name. (Refer to *Basic System Configuration Commands* in the *System Volume* for details)

### %%

This field is a preamble used to identify a vendor. It is displayed only when the output destination is log host.

### nn

This field is a version identifier of syslog. It is displayed only when the output destination is log host.

### module

The module field represents the name of the module that generates system information. You can enter the **info-center source ?** command in system view to view the module list.

### level (severity)

System information can be divided into eight levels based on its severity, from 0 to 7. Refer to Table 1-1 for definition and description of these severity levels. The levels of system information generated by modules are predefined by developers, and you cannot change the system information levels. However, you can configure to output information of the specified level using the **info-center source** command.

### digest

The digest field is a string of up to 32 characters, outlining the system information.

For system information destined to the log host:

- If the character string ends with (l), the information is log information
- If the character string ends with (t), the information is trap information
- If the character string ends with (d), the information is debugging information

For system information destined to other destinations:

- If the timestamp starts with a %, the information is log information
- If the timestamp starts with a #, the information is trap information
- If the timestamp starts with a *, the information is debugging information

**source**

This field indicates the source of the information, such as the source IP address of the log sender. This field is optional and is displayed only when the output destination is the log host.

**content**

This field provides the content of the system information.

# Configuring Information Center

## Information Center Configuration Task List

Complete the following tasks to configure information center:

| Task | Remarks |
|---|---|
| Outputting System Information to the Console | Optional |
| Outputting System Information to a Monitor Terminal | Optional |
| Outputting System Information to a Log Host | Optional |
| Outputting System Information to the Trap Buffer | Optional |
| Outputting System Information to the Log Buffer | Optional |
| Outputting System Information to the SNMP Module | Optional |
| Configuring Synchronous Information Output | Optional |

## Outputting System Information to the Console

### Outputting system information to the console

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |
| Configure the channel through which system information can be output to the console | **info-center console channel** { *channel-number* \| *channel-name* } | Optional<br>By default, system information is output to the console through channel 0 (known as console). |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the output rules of system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Configure the format of the time stamp | **info-center timestamp** { **debugging** \| **log** \| **trap** } { **boot** \| **date** \| **none** } | Optional<br>The time stamp format for log, trap and debugging information is **date** by default. |

### Enabling the display of system information on the console

After setting to output system information to the console, you need to enable the associated display function to display the output information on the console.

Follow these steps in user view to enable the display of system information on the console:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the monitoring of system information on the console | **terminal monitor** | Optional<br>Enabled on the console and disabled on the monitor terminal by default. |
| Enable the display of debugging information on the console | **terminal debugging** | Required<br>Disabled by default |
| Enable the display of log information on the console | **terminal logging** | Optional<br>Enabled by default |
| Enable the display of trap information on the console | **terminal trapping** | Optional<br>Enabled by default |

## Outputting System Information to a Monitor Terminal

System information can also be output to a monitor terminal, which is a user terminal that has login connections through the AUX, VTY user interface.

### Outputting system information to a monitor terminal

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the channel through which system information can be output to a monitor terminal | **info-center monitor channel** { *channel-number* \| *channel-name* } | Optional<br>By default, system information is output to the monitor terminal through channel 1 (known as monitor). |
| Configure the output rules of the system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Configure the format of the time stamp | **info-center timestamp** { **debugging** \| **log** \| **trap** } { **boot** \| **date** \| **none** } | Optional<br>By default, the time stamp format for log, trap and debugging information is **date**. |

### Enabling the display of system information on a monitor terminal

After setting to output system information to a monitor terminal, you need to enable the associated display function in order to display the output information on the monitor terminal.

Follow these steps to enable the display of system information on a monitor terminal:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the monitoring of system information on a monitor terminal | **terminal monitor** | Required<br>Enabled on the console and disabled on the monitor terminal by default. |
| Enable the display of debugging information on a monitor terminal | **terminal debugging** | Required<br>Disabled by default |
| Enable the display of log information on a monitor terminal | **terminal logging** | Optional<br>Enabled by default |
| Enable the display of trap information on a monitor terminal | **terminal trapping** | Optional<br>Enabled by default |

## Outputting System Information to a Log Host

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify a log host and configure the parameters when system information is output to the log host | **info-center loghost** *host-ip* [ **channel** { *channel-number* \| *channel-name* } \| **facility** *local-number* ] * | Required<br>By default, the system does not output information to a log host. If you specify to output system information to a log host, the system uses channel 2 (loghost) by default. |
| Configure the output rules of the system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Specify the source IP address for the log information | **info-center loghost source** *interface-type interface-number* | Optional<br>By default, the source interface is determined by the matched route, and the primary IP address of this interface is the source IP address of the log information. |
| Configure the format of the time stamp for system information output to the log host | **info-center timestamp loghost** { **date** \| **no-year-date** \| **none** } | Optional<br>**date** by default. |

## Outputting System Information to the Trap Buffer

**Note**

The trap buffer receives the trap information only, and discards the log and debugging information even if you have configured to output them to the trap buffer.

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |
| Configure the channel through which system information can be output to the trap buffer and specify the buffer size | **info-center trapbuffer** [ **channel** { *channel-number* \| *channel-name* } \| **size** *buffersize* ] * | Optional<br>By default, system information is output to the trap buffer through channel 3 (known as trapbuffer) and the default buffer size is 256. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the output rules of the system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Configure the format of the time stamp | **info-center timestamp** { **debugging** \| **log** \| **trap** } { **boot** \| **date** \| **none** } | Optional<br>The time stamp format for log, trap and debugging information is **date** by default. |

## Outputting System Information to the Log Buffer

**Note**

You can configure to output log, trap, and debugging information to the log buffer, but the log buffer receives the log and debugging information only, and discards the trap information.

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default. |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |
| Configure the channel through which system information can be output to the log buffer and specify the buffer size | **info-center logbuffer** [ **channel** { *channel-number* \| *channel-name* } \| **size** *buffersize* ] * | Optional<br>By default, system information is output to the log buffer through channel 4 (known as logbuffer) and the default buffer size is 512. |
| Configure the output rules of the system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Configure the format of the timestamp | **info-center timestamp** { **debugging** \| **log** \| **trap** } { **boot** \| **date** \| **none** } | Optional<br>The time stamp format for log, trap and debugging information is **date** by default. |

## Outputting System Information to the SNMP Module

**Note**

The SNMP module receives the trap information only, and discards the log and debugging information even if you have configured to output them to the SNMP module.

To monitor the device running status, trap information is usually sent to the SNMP network management station (NMS). In this case, you need to configure to send traps to the SNMP module, and then set the trap sending parameters for the SNMP module to further process traps. For details, refer to *SNMP Configuration* in the *System Volume*.

Follow these steps to configure to output system information to the SNMP module:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable information center | **info-center enable** | Optional<br>Enabled by default |
| Name the channel with a specified channel number | **info-center channel** *channel-number* **name** *channel-name* | Optional<br>Refer to Table 1-2 for default channel names. |
| Configure the channel through which system information can be output to the SNMP module | **info-center snmp channel** { *channel-number* \| *channel-name* } | Optional<br>By default, system information is output to the SNMP module through channel 5 (known as snmpagent). |
| Configure the output rules of the system information | **info-center source** { *module-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ **debug** { **level** *severity* \| **state** *state* } * \| **log** { **level** *severity* \| **state** *state* } * \| **trap** { **level** *severity* \| **state** *state* } * ] * | Optional<br>Refer to Default output rules of system information. |
| Configure the format of the timestamp | **info-center timestamp** { **debugging** \| **log** \| **trap** } { **boot** \| **date** \| **none** } | Optional<br>The time stamp format for log, trap and debugging information is **date** by default. |

## Configuring Synchronous Information Output

Synchronous information output refers to the feature that if the user's input is interrupted by system output such as log, trap, or debugging information, then after the completion of system output the system will display a command line prompt (a prompt in command editing mode, or a [Y/N] string in interaction mode) and your input so far.

This command is used in the case that your input is interrupted by a large amount of system output. With this feature enabled, you can continue your operations from where you were stopped.

Follow these steps to enable synchronous information output:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable synchronous information output | **info-center synchronous** | Required<br>Disabled by default |

**Note**

- If system information, such as log information, is output before you input any information under the current command line prompt, the system will not display the command line prompt after the system information output.
- If system information is output when you are inputting some interactive information (non Y/N confirmation information), then after the system information output, the system will not display the command line prompt but your previous input in a new line.

## Disabling a Port from Generating Link Up/Down Logging Information

By default, all the ports of the device generate link up/down logging information when the port state changes. Therefore, you may need to use this function in some cases, for example:

- You only concern the states of some of the ports. In this case, you can use this function to disable the other ports from generating link up/down logging information.
- The state of a port is not stable, and therefore redundant logging information will be generated. In this case, you can use this function to disable the port from generating link up/down logging information.

Follow the steps below to disable a port from generating link up/down logging information:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Disable the port from generating link up/down logging information | **undo enable log updown** | Required<br>By default, all ports are allowed to generate link up/down logging information when the port state changes. |

**Note**

With this feature applied to a port, when the state of the port changes, the system does not generate port link up/down logging information. In this case, you cannot monitor the port state changes conveniently. Therefore, it is recommended to use the default configuration in normal cases.

# Displaying and Maintaining Information Center

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about information channels | **display channel** [ *channel-number* \| *channel-name* ] | Available in any view |
| Display the information of each output destination | **display info-center** | Available in any view |
| Display the state of the log buffer and the log information recorded | **display logbuffer** [ **reverse** ] [ **level** *severity* \| **size** *buffersize* ] * [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | Available in any view |
| Display a summary of the log buffer | **display logbuffer summary** [ **level** *severity*] | Available in any view |
| Display the content of the log file buffer | **display logfile buffer** | Available in any view |
| Display the configuration of the log file | **display logfile summary** | Available in any view |
| Display the state of the trap buffer and the trap information recorded | **display trapbuffer** [ **reverse** ] [ **size** *buffersize* ] | Available in any view |
| Reset the log buffer | **reset logbuffer** | Available in user view |
| Reset the trap buffer | **reset trapbuffer** | Available in user view |

# Information Center Configuration Examples

## Outputting Log Information to a Unix Log Host

### Network requirements

- Send log information to a Unix log host with an IP address of 1.2.0.1/16;
- Log information with severity higher than informational will be output to the log host;
- The source modules are ARP and IP.

**Figure 1-1** Network diagram for outputting log information to a Unix log host


### Configuration procedure

Before the configuration, make sure that there is a route between Device and PC.

1) Configure the device

# Enable information center.

```
<Sysname> system-view
[Sysname] info-center enable
```

# Specify the host with IP address 1.2.0.1/16 as the log host, use channel **loghost** to output log information (optional, **loghost** by default), and use **local4** as the logging facility.

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local4
```

# Disable the output of log, trap, and debugging information of all modules on channel **loghost**.

```
[Sysname] info-center source default channel loghost debug state off log state off trap state off
```

---

**Caution**

As the default system configurations for different channels are different, you need to disable the output of log, trap, and debugging information of all modules on the specified channel (**loghost** in this example) first and then configure the output rule as needed so that unnecessary information will not be output.

---

# Configure the information output rule: allow log information of ARP and IP modules with severity equal to or higher than **informational** to be output to the log host. (Note that the source modules allowed to output information depend on the device model.)

```
[Sysname] info-center source arp channel loghost log level informational state on
[Sysname] info-center source ip channel loghost log level informational state on
```

2) Configure the log host

The following configurations were performed on SunOS 4.0 which has similar configurations to the Unix operating systems implemented by other vendors.

Step 1: Log in to the log host as a root user.

Step 2: Create a subdirectory named **Device** under directory **/var/log/**, and create file **info.log** under the **Device** directory to save logs of **Device**.

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

Step 3: Edit file **/etc/syslog.conf** and add the following contents.

```
# Device configuration messages
local4.info    /var/log/Device/info.log
```

In the above configuration, **local4** is the name of the logging facility used by the log host to receive logs. **info** is the information level. The Unix system will record the log information with severity level equal to or higher than **informational** to file **/var/log/Device/info.log**.

**Note**

Be aware of the following issues while editing file **/etc/syslog.conf**:

- Comments must be on a separate line and begin with the # sign.
- No redundant spaces are allowed after the file name.
- The logging facility name and the information level specified in the **/etc/syslog.conf** file must be identical to those configured on the device using the **info-center loghost** and **info-center source** commands; otherwise the log information may not be output properly to the log host.

Step 4: After log file **info.log** is created and file **/etc/syslog.conf** is modified, you need to issue the following commands to display the process ID of **syslogd**, kill the **syslogd** process and then restart **syslogd** using the **–r** option to make the modified configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

After the above configurations, the system will be able to record log information into the log file.

## Outputting Log Information to a Linux Log Host

### Network requirements

- Send log information to a Linux log host with an IP address of 1.2.0.1/16;
- Log information with severity higher than informational will be output to the log host;
- All modules can output log information.

**Figure 1-2** Network diagram for outputting log information to a Linux log host


### Configuration procedure

Before the configuration, make sure that there is a route between Device and PC.

1) Configure the device

# Enable information center.

```
<Sysname> system-view
[Sysname] info-center enable
```

# Specify the host with IP address 1.2.0.1/16 as the log host, use channel **loghost** to output log information (optional, **loghost** by default), and use **local5** as the logging facility.

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local5
```

# Disable the output of log, trap, and debugging information of all modules on channel **loghost**.

```
[Sysname] info-center source default channel loghost debug state off log state off trap state off
```

---

**Caution**

As the default system configurations for different channels are different, you need to disable the output of log, trap, and debugging information of all modules on the specified channel (**loghost** in this example) first and then configure the output rule as needed so that unnecessary information will not be output.

---

# Configure the information output rule: allow log information of all modules with severity equal to or higher than **informational** to be output to the log host.

```
[Sysname] info-center source default channel loghost log level informational state on
```

2) Configure the log host

Step 1: Log in to the log host as a root user.

Step 2: Create a subdirectory named **Device** under directory **/var/log/**, and create file **info.log** under the **Device** directory to save logs of **Device**.

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

Step 3: Edit file **/etc/syslog.conf** and add the following contents.

```
# Device configuration messages
local5.info    /var/log/Device/info.log
```

In the above configuration, **local5** is the name of the logging facility used by the log host to receive logs. **info** is the information level. The Linux system will record the log information with severity level equal to or higher than **informational** to file **/var/log/Device/info.log**.

---

**Note**

Be aware of the following issues while editing file **/etc/syslog.conf**:

- Comments must be on a separate line and begin with the # sign.
- No redundant spaces are allowed after the file name.
- The logging facility name and the information level specified in the **/etc/syslog.conf** file must be identical to those configured on the device using the **info-center loghost** and **info-center source** commands; otherwise the log information may not be output properly to the log host.

---

Step 4: After log file **info.log** is created and file **/etc/syslog.conf** is modified, you need to issue the following commands to display the process ID of **syslogd**, kill the **syslogd** process, and restart **syslogd** using the **-r** option to make the modified configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -9 147
```

```
# syslogd -r &
```

**Note**

Ensure that the **syslogd** process is started with the -r option on a Linux log host.

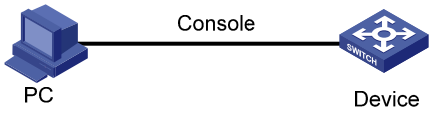
After the above configurations, the system will be able to record log information into the log file.

## Outputting Log Information to the Console

### Network requirements

- Log information with a severity higher than informational will be output to the console;
- The source modules are ARP and IP.

**Figure 1-3** Network diagram for sending log information to the console




### Configuration procedure

# Enable information center.

```
<Sysname> system-view
[Sysname] info-center enable
```

# Use channel **console** to output log information to the console (optional, **console** by default).

```
[Sysname] info-center console channel console
```

# Disable the output of log, trap, and debugging information of all modules on channel **console**.

```
[Sysname] info-center source default channel console debug state off log state off trap state off
```

**Caution**

As the default system configurations for different channels are different, you need to disable the output of log, trap, and debugging information of all modules on the specified channel (**console** in this example) first and then configure the output rule as needed so that unnecessary information will not be output.

# Configure the information output rule: allow log information of ARP and IP modules with severity equal to or higher than **informational** to be output to the console. (Note that the source modules allowed to output information depend on the device model.)

```
[Sysname] info-center source arp channel console log level informational state on
[Sysname] info-center source ip channel console log level informational state on
[Sysname] quit
```

# Enable the display of log information on a terminal. (Optional, this function is enabled by default.)

```
<Sysname> terminal monitor
% Current terminal monitor is on
<Sysname> terminal logging
% Current terminal logging is on
```

After the above configuration takes effect, if the specified module generates log information, the information center automatically sends the log information to the console, which then displays the information.

# Table of Contents

# 1 PoE Configuration

When configuring PoE, go to these sections for information you are interested in:



## PoE Overview

### Introduction to PoE

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PD) such as IP telephone, wireless LAN access point, and web camera from Ethernet interfaces through twisted pair cables.

#### Advantages

- Reliable: Power is supplied in a centralized way so that it is very convenient to provide a backup power supply.
- Easy to connect: A network terminal requires only one Ethernet cable, but no external power supply.
- Standard: In compliance with IEEE 802.3af, and a globally uniform power interface is adopted.
- Promising: It can be applied to IP telephones, wireless LAN access points, portable chargers, card readers, web cameras, and data collectors.

#### Composition

A PoE system consists of PoE power, PSE, and PD.

- PoE power

The whole PoE system is powered by the PoE power, which includes external PoE power and internal PoE power.

- PSE

PSE detecting that a PD is unplugged, the PSE stops supplying power to the PD.

An Ethernet interface with the PoE capability is called PoE interface. Currently, a PoE interface can be an FE or GE interface.

- PD

A PD is a device accepting power from the PSE. There are standard PDs and nonstandard PDs. A standard PD refers to the one that complies with IEEE 802.3af. The PD that is being powered by the PSE can be connected to other power supply units for redundancy backup.

### Protocol Specification

The protocol specification related to PoE is IEEE 802.3af.

## PoE Configuration Task List

Complete these tasks to configure PoE:

| Task | Remarks |
|---|---|
| Configuring the PoE Interface | Required |
| Configuring PoE Power Management | Optional |
| Configuring the PoE Monitoring Function | Optional |
| Upgrading PSE Processing Software Online | Optional |
| Configuring a PD Disconnection Detection Mode | Optional |
| Enabling the PSE to Detect Nonstandard PDs | Optional |

**Caution**

- When the PoE power or PSE fails, you cannot configure PoE.
- Turning off of the PoE power during the startup of the device might result in the failure to restore the PoE configuration.

## Configuring the PoE Interface

You can configure a PoE interface in either of the following two ways:

- Adopting the command line.
- Configuring a PoE configuration file and applying the file to the specified PoE interface(s).

Usually, you can adopt the command line to configure a single PoE interface, and adopt a PoE configuration file to configure multiple PoE interfaces at the same time.

**Caution**

You can adopt either mode to configure, modify, or delete a PoE configuration parameter under the same PoE interface.

The PSE supplies power for a PoE interface in the following two modes:

- Signal cables modes: PSE uses the twisted pairs (1, 2, 3, and 6) of category-3/5 cables, which are used for data transmission, to power the PD simultaneously.

- Spare cables modes: PSE uses the twisted pairs (4, 5, 7 and 8) of category-3/5 cables, which are spare during data transmission, to power the PD.

---

 **Note**

3Com Switch 4500G only support for signal mode.

---

## Configuring a PoE Interface through the Command Line

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter PoE interface view | **interface** *interface-type interface-number* | — |
| Enable PoE | **poe enable** | Required<br>Disabled by default. |
| Configure the maximum power for the PoE interface | **poe max-power** *max-power* | Optional<br>15,400 milliwatts by default. |
| Configure the PoE mode for the PoE interface | **poe mode signal** | Optional<br>**signal** (power over signal cables) by default. |
| Configure a description for the PD connected to the PoE interface | **poe pd-description** *string* | Optional<br>By default, no description for the PD connected to the PoE interface is available. |

## Configuring PoE Interfaces Through a PoE Configuration File

A PoE configuration file is used to configure at the same time multiple PoE interfaces with the same attributes to simplify operations. This configuration method is a supplement to the command line configuration.

The PoE configuration file features:

- You can create multiple PoE configuration files for different user group and apply the specific PoE configuration file to the port a user group uses.
- When you use a PD on a port with PoE configuration file being applied, the configuration in the PoE configuration file will be enabled.

Commands in a PoE configuration file are called configurations.

Follow these steps to configure PoE interfaces through a PoE configuration file:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a PoE configuration file and enter PoE configuration file view | | **poe-profile** *profile-name* [ *index* ] | Required |
| Enable PoE for the PoE interface | | **poe enable** | Required<br>Disabled by default. |
| Configure the maximum power for the PoE interface | | **poe max-power** *max-power* | Optional<br>15,400 milliwatts by default. |
| Configure the PoE mode for the PoE interface | | **poe mode signal** | Optional<br>**signal** (power over signal cables) by default. |
| Return to system view | | **quit** | — |
| Apply the PoE configuration file to the PoE interface (s) | Apply the PoE configuration file to one or more PoE interfaces | **apply poe-profile** { **index** *index* \| **name** *profile-name* } **interface** *interface-range* | Use either approach |
| | Apply the PoE configuration file to the current PoE interface in PoE interface view | **interface** *interface-type interface-number* | |
| | | **apply poe-profile** { **index** *index* \| **name** *profile-name* } | |

**Caution**

- After a PoE configuration file is applied to a PoE interface, other PoE configuration files can not take effect on this PoE interface.
- If a PoE configuration file is already applied to a PoE interface, you must execute the **undo apply poe-profile** command to remove the application to the interface before deleting or modifying the PoE configuration file.
- If you have configured a PoE interface through the command line, you cannot configure it through a PoE configuration file again. If you want to reconfigure the interface through a PoE configuration file, you must first remove the command line configuration on the PoE interface.
- You must use the same mode (command line or PoE configuration file) to configure the **poe max-power** *max-power* and **poe priority** { **critical** | **high** | **low** } commands.

# Configuring PoE Power Management

## Configuring PD Power Management

The power priority of a PD depends on the priority of the PoE interface. The priority levels of PoE interfaces include critical, high and low in descending order. Power supply to a PD is subject to PD power management policies.

All PSEs implement the same PD power management policies. When the PSE supplies power to a PD,

- By default, no power will be supplied to a new PD if the PSE power is overloaded.
- Under the control of a priority policy, the PD with a lower priority is first powered off to guarantee the power supply to the new PD with a higher priority when the PSE power is overloaded.

---

**Note**

- 19 watts guard band is reserved for each PoE interface on the device to prevent a PD from being powered off because of sudden increase of the power of the PD. When the remaining power of the interface is lower than 19 watts and no priority is configured for a PoE interface, the PSE does not supply power to the new PD; when the remaining power of the interface is lower than 19 watts, but priority is configured for a PoE interface, the interface with a higher priority can preempt the power of the interface with a lower priority to ensure the normal working of the higher priority interface.
- If the sudden increase of the power of the PD results in PSE power overload, power supply to the PD on the PoE interface with a lower priority will be stopped.

---

If the guaranteed remaining PSE power (maximum PSE power – power allocated to the critical PoE interface, regardless of whether PoE is enabled for the PoE interface) is lower than the maximum power of the PoE interface, you will fail to set the priority of the PoE interface to **critical**. Otherwise, you can succeed in setting the priority to **critical**, and this PoE interface will preempt the power of other PoE interfaces with a lower priority level. In the latter case, the PoE interfaces whose power is preempted will be powered off, but their configurations will remain unchanged. When you change the priority of a PoE interface from critical to a lower level, the PDs connecting to other PoE interfaces will have an opportunity of being powered.

### Configuration prerequisites

Enable PoE for PoE interfaces.

### Configuration procedure

Follow these steps to configure PD power management:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure the power priority for a PoE interface | Configure the power priority for the PoE interface in PoE interface view | **interface** *interface-type interface-number* | Use either command.<br>By default, the power priority of a PoE interface is **low**. |
| | | **poe priority** { **critical** \| **high** \| **low** } | |
| | Configure the power priority for the PoE interface in PoE configuration file view | **poe-profile** *profile-name* [ *index* ] | |
| | | **poe priority** { **critical** \| **high** \| **low** } | |
| Configure a PD power management priority policy | | **poe pd-policy priority** | Optional<br>By default, no PD power management priority policy is configured. |

# Configuring the PoE Monitoring Function

The PoE monitoring function involves monitoring of PoE power, PSE and PD.

- Monitoring PoE power means monitoring the voltage of the PoE power.
- When the current power utilization of the PSE is above or below the alarm threshold for the first time, the system will send a Trap message.
- When the PSE starts or stops supplying power to a PD, the system will send a Trap message, too.

## Configuring a Power Alarm Threshold for the PSE

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a power alarm threshold for the PSE | **poe utilization-threshold** *utilization-threshold-value* **pse** *pse-id* | Optional<br>80% by default. |

# Upgrading PSE Processing Software Online

You can upgrade the PSE processing software online in either of the following two modes:

- refresh mode

This mode enables you to update the PSE processing software without deleting it.

- full mode

This mode deletes the PSE processing software and reloads it. When the PSE processing software is damaged (in this case, you can execute none of PoE commands successfully), you can upgrade the PSE software processing software in full mode to restore the PSE function.

Online PSE processing software upgrade may be unexpectedly interrupted (for example, an error results in device reboot). If you fail to upgrade the PSE processing software in full mode after reboot,

you can power off the device and restart it before upgrading it again. After upgrade, restart the device manually to make the original PoE configurations take effect.

Follow these steps to upgrade the PSE processing software online:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Upgrade the PSE processing software online | **poe update** { **full** \| **refresh** } *filename* **pse** *pse-id* | Optional |

## Configuring a PD Disconnection Detection Mode

To detect the PD connection with PSE, PoE provides two detection modes: AC detection and DC detection. The AC detection mode is energy saving relative to the DC detection mode.

Follow these steps to configure a PD disconnection detection mode:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a PD disconnection detection mode | **poe disconnect** { **ac** \| **dc** } | Optional<br>The default PD disconnection detection mode varies with devices. |

**Caution**

If you adjust the PD disconnection detection mode when the device is running, the connected PDs will be powered off. Therefore, be cautious to do so.

## Enabling the PSE to Detect Nonstandard PDs

There are standard PDs and nonstandard PDs. Usually, the PSE can detect only standard PDs and supply power to them. The PSE can detect nonstandard PDs and supply power to them only after the PSE is enabled to detect nonstandard PDs.

Follow these steps to enable the PSE to detect nonstandard PDs:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the PSE to detect nonstandard PDs | **poe legacy enable pse** *pse-id* | Optional<br>Disabled by default. |

# Displaying and Maintaining PoE

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the mapping between ID, module, and member ID of all PSEs. | **display poe device** | Available in any view |
| Display the power state and information of the specified PoE interface | **display poe interface** [ *interface-type interface-number* ] | |
| Display the power information of a PoE interface(s) | **display poe interface power** [ *interface-type interface-number* ] | |
| Display the information of PSE | **display poe pse** [ *pse-id* ] | |
| Display the power state and information of all PoE interfaces connected with the PSE | **display poe pse** *pse-id* **interface** | |
| Display the power of all PoE interfaces connected with the PSE | **display poe pse** *pse-id* **interface power** | |
| Display all information of the configurations and applications of the PoE configuration file | **display poe-profile** [ **index** *index* \| **name** *profile-name* ] | |
| Display all information of the configurations and applications of the PoE configuration file applied to the specified PoE interface | **display poe-profile interface** *interface-type interface-number* | |

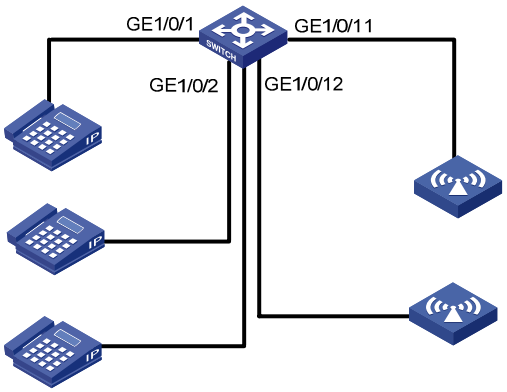
# PoE Configuration Example

## Network requirements

The device provides power supply for PDs through PoE interfaces.

- GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are connected to IP telephones.
- GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 are connected to access point (AP) devices.
- The power priority of GigabitEthernet 1/0/2 is critical.
- The power of the AP device connected to GigabitEthernet 1/0/11 does not exceed 9,000 milliwatts.

**Figure 1-1** Network diagram for PoE




### Configuration procedure

# Enable PoE on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/11, and GigabitEthernet 1/0/12.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe enable
[Sysname-GigabitEthernet1/0/11] quit
[Sysname] interface GigabitEthernet 1/0/12
[Sysname-GigabitEthernet1/0/12] poe enable
[Sysname-GigabitEthernet1/0/12] quit
```

# Set the power priority level of GigabitEthernet 1/0/2 to **critical**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe priority critical
[Sysname-GigabitEthernet1/0/2] quit
# Set the maximum power of GigabitEthernet 1/0/11 to 9,000 milliwatts.
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe max-power 9000
[Sysname-GigabitEthernet1/0/11] quit
```

After the configuration takes effect, the IP phone and AR device are powered and can work normally.

## Troubleshooting PoE

**Symptom 1**: Setting of the priority of a PoE interface to **critical** fails.

**Analysis**:

- The guaranteed remaining power of the PSE is lower than the maximum power of the PoE interface.

- The priority of the PoE interface is already set.

**Solution**:

- In the first case, you can solve the problem by increasing the maximum PSE power, or by reducing the maximum power of the PoE interface when the guaranteed remaining power of the PSE cannot be modified.
- In the second case, you should first remove the priority already configured.

**Symptom 2**: Applying a PoE configuration file to a PoE interface fails.

**Analysis**:

- Some configurations in the PoE configuration file are already configured.
- Some configurations in the PoE configuration file do not meet the configuration requirements of the PoE interface.
- Another PoE configuration file is already applied to the PoE interface.

**Solution**:

- In the first case, you can solve the problem by removing the original configurations of those configurations.
- In the second case, you need to modify some configurations in the PoE configuration file.
- In the third case, you need to remove the application of the undesired PoE configuration file to the PoE interface.

**Symptom 3**: Provided that parameters are valid, configuring an AC input under-voltage threshold fails.

**Analysis**:

The AC input under-voltage threshold is greater than or equal to the AC input over-voltage threshold.

**Solution**:

You can drop the AC input under-voltage threshold below the AC input over-voltage threshold.

# Table of Contents

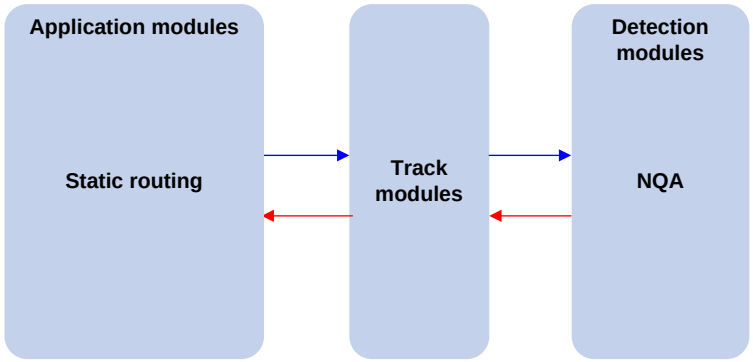
# 1 Track Configuration

When configuring Track, go to these sections for information you are interested in:



## Track Overview

**Figure 1-1** Collaboration through the Track module




The Track module is used to implement collaboration between different modules.

The collaboration here involves three parts: the application modules, the Track module, and the detection modules. These modules collaborate with one another through collaboration objects. That is, the detection modules trigger the application modules to perform certain operations through the Track module. More specifically, the detection modules probe the link status, network performance and so on, and inform the application modules of the detection result through the Track module. After the application modules are aware of the changes of network status, they deal with the changes accordingly to avoid communication interruption and network performance degradation.

The Track module works between the application modules and the detection modules and is mainly used to obscure the difference of various detection modules to provide a unified interface for application modules.

### Collaboration Between the Track Module and the Detection Modules

You can establish the collaboration between the Track module and the detection modules through configuration. A detection module probes the link status and informs the Track module of the probe result. The Track module then changes the status of the Track object accordingly:

- If the probe succeeds, the status of the corresponding Track object is **Positive**;
- If the probe fails, the status of the corresponding Track object is **Negative**.

At present, the detection modules that can collaborate with the Track module is the Network Quality Analyzer (NQA). Refer to *NQA Configuration* in the *System Volume* for details of NQA.

### Collaboration Between the Track Module and the Application Modules

You can establish the collaboration between the Track module and the application modules through configuration. If the status of the Track object changes, the Track module tells the application modules to deal with the change accordingly.

At present, the application modules that can collaborate with the Track module is Static routing.

## Track Configuration Task List

To implement the collaboration function, you need to establish collaboration between the Track module and the detection modules, and between the Track module and the application modules.

Complete these tasks to configure Track module:

| Task | | Remarks |
|---|---|---|
| Configuring Collaboration Between the Track Module and the Detection Modules | Configuring Track-NQA Collaboration | Required |
| Configuring Collaboration Between the Track Module and the Application Modules | Configuring Track-Static Routing Collaboration | Required |

## Configuring Collaboration Between the Track Module and the Detection Modules

### Configuring Track-NQA Collaboration

Through the following configuration, you can establish the collaboration between the Track module and the NQA, which probes the link status and informs the Track module of the probe result.

Follow these steps to configure Track-NQA collaboration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a Track object and associate it with the specified Reaction entry of the NQA test group | **track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-num* | Required<br>No Track object is created by default. |

**Caution**

When you configure a Track object, the specified NQA test group and Reaction entry can be nonexistent. In this case, the status of the configured Track object is **Invalid**.

# Configuring Collaboration Between the Track Module and the Application Modules

## Configuring Track-Static Routing Collaboration

You can check the validity of a static route in real time by establishing collaboration between Track and static routing.

If you specify the next hop but not the egress interface when configuring a static route, you can associate the static route with a Track object and thus check the validity of the static route according to the status of the Track object.

- If the status of the Track object is **Positive**, then the next hop of the static route is reachable, and the configured static route is valid.
- If the status of the Track object is **Negative**, then the next hop of the static route is unreachable, and the configured static route is invalid.

Follow these steps to configure the Track-Static Routing collaboration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the Track-Static Routing collaboration, so as to check the reachability of the next hop of the static route | **ip route-static** *dest-address* { *mask* \| *mask-length* } *next-hop-address* **track** *track-entry-number* [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **description** *description-text* ] | Required<br>Not configured by default. |

**Note**

- For the configuration of Track-Static Routing collaboration, the specified static route can be an existent or nonexistent one. For an existent static route, the static route and the specified Track object are associated directly; for a nonexistent static route, the system creates the static route and then associates it with the specified Track object.
- The Track object to be associated with the static route can be a nonexistent one. After you use the **track** command to create the Track object, the association takes effect.
- If a static route needs route recursion, the associated Track object must monitor the next hop of the recursive route instead of that of the static route; otherwise, a valid route may be considered invalid.
- For details of static route configuration, refer to *Static Routing Configuration* in the *IP Routing Volume*.

# Displaying and Maintaining Track Object(s)

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about the specified Track object or all Track objects | **display track** { track-entry-number \| all } | Available in any view |

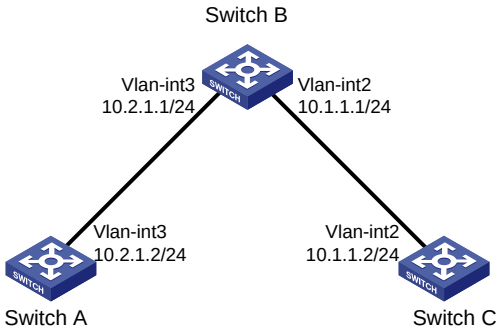
# Track Configuration Examples

## Static Routing-Track-NQA Collaboration Configuration Example

### Network requirements

- The next hop of the static route from Switch A to Switch C is Switch B.
- Configure Static Routing-Track-NQA collaboration on Switch A to implement real-time monitoring of the validity of the static route to Switch C.

**Figure 1-2** Network diagram for Static Routing-Track-NQA collaboration configuration




### Configuration procedure

1) Configure the IP address of each interface as shown in Figure 1-2.
2) Configure a static route on Switch A and associate it with the Track object.

# Configure the address of the next hop of the static route to Switch C as 10.2.1.1, and configure the static route to associate with Track object 1.

```
<SwitchA> system-view
[SwitchA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

3) Configure an NQA test group on Switch A.

# Create an NQA test group with the administrator **admin** and the operation tag **test**.

```
[SwitchA] nqa entry admin test
```

# Configure the test type as ICMP-echo.

```
[SwitchA-nqa-admin-test] type icmp-echo
```

# Configure the destination address as 10.2.1.1

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.1
```

# Configure the test frequency as 100 ms.

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

# Configure Reaction entry 1, specifying that five consecutive probe failures trigger the Static Routing-Track-NQA collaboration.

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

# Start NQA probes.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

4) Configure a Track object on Switch A.

# Configure Track object 1, and associate it with Reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test)**.

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

5) Verify the configuration

# Display information of the Track object on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.1.1.0/24         Static 60   0            10.2.1.1        Vlan3
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output information above indicates the NQA test result, that is, the next hop 10.2.1.1 is reachable (the status of the Track object is **Positive**), and the configured static route is valid.

# Remove the IP address of interface VLAN-interface 3 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] undo ip address
```

# Display information of the Track object on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Negative
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 4        Routes : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output information above indicates the NQA test result, that is, the next hop 10.2.1.1 is unreachable (the status of the Track object is **Negative**), and the configured static route is invalid.

# Table of Contents

# 1 NQA Configuration

When configuring NQA, go to these sections for information you are interested in:



## NQA Overview

### Introduction to NQA

Network Quality Analyzer (NQA) analyzes network performance, services and service quality through sending test packets, and provides you with network performance and service quality parameters such as jitter, TCP connection delay, FTP connection delay and file transfer rate.

With the NQA test results, you can:

1) Know network performance in time and then take corresponding measures.
2) Diagnose and locate network faults.

### Features of NQA

#### Supporting multiple test types

Ping can use only the Internet Control Message Protocol (ICMP) to test the reachability of the destination host and the roundtrip time of a packet to the destination. As an enhancement to the Ping tool, NQA provides multiple test types and more functions.

At present, NQA supports ten test types: ICMP echo, DHCP, FTP, HTTP, UDP jitter, SNMP, TCP, UDP echo, voice and DLSw.

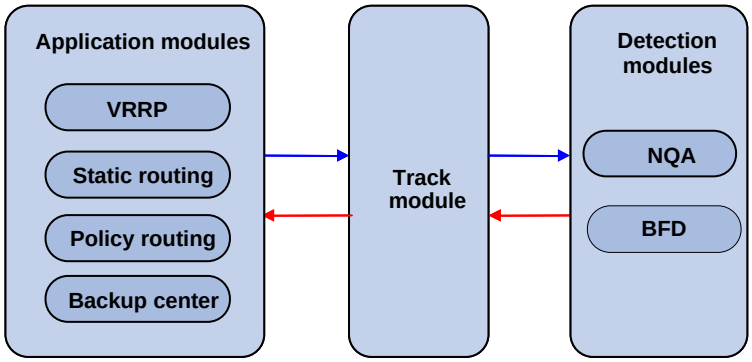
In an NQA test, the client sends different types of test packets to the peer to detect the availability and the response time of the peer, helping you know protocol availability and network performance based on the test results.

#### Supporting the collaboration function

Collaboration is implemented by establishing collaboration objects to monitor the detection results of the current test group. If the number of consecutive probe failures reaches a certain limit, NQA's

collaboration with other modules is triggered. The implementation of collaboration is shown in Figure 1-1.

**Figure 1-1** Implementation of collaboration




The collaboration here involves three parts: the application modules, the Track module, and the detection modules.

- The detection modules monitor the link status, network performance and so on, and inform the Track module of the detection result.
- Upon receiving the detection result, the Track module changes the status of the Track object accordingly and informs the application modules. The Track module works between the application modules and the detection modules and is mainly used to obscure the difference of various detection modules to provide a unified interface for application modules.
- The application modules then deal with the changes accordingly based on the status of the Track object, and thus collaboration is implemented.

Take static routing as an example. You have configured a static route with the next hop 192.168.0.88. If 192.168.0.88 is reachable, the static route is valid; if 192.168.0.88 is unreachable, the static route is invalid. With the collaboration between NQA, Track module and application modules, real time monitoring of reachability of the static route can be implemented:

1) Monitor reachability of the destination 192.168.0.88 through NQA.
2) If 192.168.0.88 is detected to be unreachable, NQA will inform the static routing module through Track module.
3) The static routing module then can know that the static route is invalid.

---

**Note**

- At present, VRRP, policy routing and backup center are not supported.
- For the detailed description of the Track module, see *Track Configuration* in the *System Volume*.

---

## Supporting delivery of traps

You can set whether to send traps to the network management server when an NQA test is performed. When a probe fails or a test is completed, the network management server can be notified, and the network administrator can know the network running status and performance in time through the traps sent.

## Basic Concepts of NQA

### Test group

Before performing an NQA test, you need to create an NQA test group, and configure NQA test parameters such as test type, destination address and destination port.

Each test group has an administrator name and operation tag, which can uniquely define a test group.

### Test and probe

After an NQA test is started, one test is performed at a regular interval and you can set the interval as needed.

One NQA test involves multiple consecutive probes and you can set the number of the probes.

---

**Note**

Only one probe can be made in one voice test.

---

In different test types, probe has different meanings:

- For a TCP or DLSw test, one probe means one connection;
- For a UDP jitter or a voice test, multiple packets are sent successively in one probe, and the number of packets sent in one probe depends on the configuration of the **probe packet-number** command;
- For an FTP, HTTP or DHCP test, one probe means to carry out a corresponding function;
- For an ICMP echo or UDP echo test, one packet is sent in one probe;
- For an SNMP test, three packets are sent in one probe.

### NQA client and server

NQA client is the device initiating an NQA test and the NQA test group is created on the NQA client.

NQA server processes the test packets sent from the NQA client, as shown in Figure 1-2. The NQA server makes a response to the request originated by the NQA client by listening to the specified destination address and port number.

**Figure 1-2** Relationship between the NQA client and NQA server


In most NQA tests, you only need to configure the NQA client; while in TCP, UDP echo, UDP jitter, and voice tests, you must configure the NQA server.

You can create multiple TCP or UDP listening services on the NQA server, with each listening service corresponding to a specified destination address and port number. The IP address and port number specified for a listening service on the server must be consistent with those on the client and must be different from those of an existing listening service.

### NQA Test Operation

An NQA test operation is as follows:

1) The NQA client constructs packets with the specified type, and sends them to the peer device;
2) Upon receiving the packet, the peer device replies with a response with a timestamp.
3) The NQA client computes the packet loss rate and RTT based on whether it has received the response and the timestamp in the response.

## NQA Configuration Task List

For TCP, UDP jitter, UDP echo or voice tests, you need to configure the NQA server on the peer device.

Follow these steps to enable the NQA server:

| Task | Remarks |
|---|---|
| Configuring the NQA Server | Required for TCP, UDP echo, UDP jitter and voice tests |

To perform an NQA test successfully, make the following configurations on the NQA client:

1) Enable the NQA client;
2) Create a test group and configure test parameters according to the test type. The test parameters may vary with test types;
3) Start the NQA test;

After the test, you can view test results using the **display** or **debug** commands.

Complete these tasks to configure NQA client:

| Task | | Remarks |
|---|---|---|
| Enabling the NQA Client | | Required |
| Creating an NQA Test Group | | Required |
| Configuring an NQA Test Group | Configuring an ICMP Echo Test | Required<br>Use any of the approaches |
| | Configuring a DHCP Test | |
| | Configuring an FTP Test | |
| | Configuring an HTTP Test | |
| | Configuring a UDP Jitter Test | |
| | Configuring an SNMP Test | |
| | Configuring a TCP Test | |
| | Configuring a UDP Echo Test | |
| | Configuring a Voice Test | |
| | Configuring a DLSw Test | |
| Configuring the Collaboration Function | | Optional |
| Configuring Trap Delivery | | Optional |
| Configuring the NQA Statistics Function | | Optional |

| Task | Remarks |
|---|---|
| Configuring Optional Parameters Common to an NQA Test Group | Optional |
| Scheduling an NQA Test Group | Required |

## Configuring the NQA Server

Before performing TCP, UDP echo, UDP jitter or voice tests, you need to configure the NQA server on the peer device. The NQA server makes a response to the request originated by the NQA client by listening to the specified destination address and port number.

Follow these steps to configure the NQA server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the NQA server | **nqa server enable** | Required<br>Disabled by default. |
| Configure the UDP or TCP listening function on the NQA server | **nqa server** { **tcp-connect** \| **udp-echo** } *ip-address port-number* | Required<br>The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service. |

## Enabling the NQA Client

Configurations on the NQA client take effect only when the NQA client is enabled.

Follow these steps to enable the NQA client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the NQA client | **nqa agent enable** | Optional<br>Enabled by default. |

## Creating an NQA Test Group

One test corresponds to one test group. You can configure test types after you create a test group and enter the test group view.

Follow theses steps to create an NQA test group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an NQA test group and enter the NQA test group view | **nqa entry** *admin-name operation-tag* | Required |

**Note**

If you execute the **nqa entry** command to enter the test group view with test type configured, you will enter the test type view of the test group directly.

# Configuring an NQA Test Group

## Configuring an ICMP Echo Test

An ICMP echo test is used to test reachability of the destination host according to the ICMP echo reply or timeout information. An ICMP echo test has the same function with the **ping** command but has more abundant output information. You can use the ICMP echo test to locate connectivity problems in a network.

Follow these steps to configure an ICMP echo test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as ICMP echo and enter test type view | **type icmp-echo** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation. |
| Configure the size of probe packets sent | **data-size** *size* | Optional<br>100 bytes by default. |
| Configure the filler string of a probe packet sent | **data-fill** *string* | Optional<br>By default, the filler string of a probe packet is the hexadecimal number 00010203040506070809. |
| Specify the IP address of an interface as the source IP address of an ICMP echo request | **source interface** *interface-type interface-number* | Optional<br>By default, no interface address is specified as the source IP address of ICMP probe requests.<br>If you use the **source ip** command to configure the source IP address of ICMP echo probe requests, the **source interface** command is invalid.<br>The interface specified by this command must be up. Otherwise, the probe will fail. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the source IP address of a probe request | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>If no source IP address is specified, but the source interface is specified, the IP address of the source interface is taken as the source IP address of ICMP probe requests.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the probe will fail. |
| Configure the next hop IP address for an ICMP echo request | **next-hop** *ip-address* | Optional<br>By default, no next hop IP address is configured. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

## Configuring a DHCP Test

A DHCP test is mainly used to test the existence of a DHCP server on the network as well as the time necessary for the DHCP server to respond to a client request and assign an IP address to the client.

### Configuration prerequisites

Before performing a DHCP test, you need to configure the DHCP server. If the NQA (DHCP client) and the DHCP server are not in the same network segment, you need to configure a DHCP relay. For the configuration of DHCP server and DHCP relay, see *DHCP Configuration* in the *IP Services Volume*.

### Configuring a DHCP test

Follow these steps to configure a DHCP test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as DHCP and enter test type view | **type dhcp** | Required |
| Specify an interface for a DHCP test | **operation interface** *interface-type interface-number* | Required<br>By default, no interface is specified to perform a DHCP test.<br>The interface specified by the **source interface** command must be up; otherwise, the test fails. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

**Note**

- As DHCP test is a process to simulate address allocation in DHCP, the IP address of the interface performing the DHCP test will not be changed.
- After the DHCP test is completed, the NQA client will send a DHCP-RELEASE packet to release the obtained IP address.

## Configuring an FTP Test

An FTP test is mainly used to test the connection between the NQA client and a specified FTP server and the time necessary for the FTP client to transfer a file to or download a file from the FTP server.

### Configuration prerequisites

Before an FTP test, you need to perform some configurations on the FTP server. For example, you need to configure the username and password used to log onto the FTP server. For the FTP server configuration, see *File System Management Configuration* in the *System Volume*.

### Configuring an FTP test

Follow these steps to configure an FTP test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as FTP and enter test type view | **type ftp** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination IP address for a test operation is the IP address of the FTP server. |
| Configure the source IP address of a probe request | **source ip** *ip-address* | Required<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the operation type | **operation** { **get** \| **put** } | Optional<br>By default, the operation type for the FTP is **get**, that is, obtaining files from the FTP server. |
| Configure a login username | **username** *name* | Required<br>By default, no login username is configured. |
| Configure a login password | **password** *password* | Required<br>By default, no login password is configured. |
| Specify a file to be transferred between the FTP server and the FTP client | **filename** *file-name* | Required<br>By default, no file is specified. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

**Note**

- When you execute the **put** command, a file *file-name* with fixed size and content is created on the FTP server; when you execute the **get** command, the device does not save the files obtained from the FTP server.
- When you execute the **get** command, the FTP test cannot succeed if a file named *file-name* does not exist on the FTP server.
- When you execute the **get** command, please use a file with a smaller size as a big file may result in test failure because of timeout, or may affect other services because of occupying too much network bandwidth.

## Configuring an HTTP Test

An HTTP test is used to test the connection between the NQA client and a specified HTTP server and the time required to obtain data from the HTTP server, thus detecting the connectivity and performance of the HTTP server.

### Configuration prerequisites

Before performing an HTTP test, you need to configure the HTTP server.

### Configuring an HTTP test

Follow these steps to configure an HTTP test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the test type as HTTP and enter test type view | **type http** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination IP address for a test operation is the IP address of the HTTP server. |
| Configure the source IP address of a probe request | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure the operation type | **operation** { **get** \| **post** } | Optional<br>By default, the operation type for the HTTP is **get**, that is, obtaining data from the HTTP server. |
| Configure the website that an HTTP test visits | **url** *url* | Required |
| Configure the HTTP version used in the HTTP test | **http-version v1.0** | Optional<br>By default, HTTP 1.0 is used in an HTTP test. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

**Note**

The TCP port number for the HTTP server must be 80 in an HTTP test. Otherwise, the test will fail.

## Configuring a UDP Jitter Test

**Note**

It is recommended not to perform an NQA UDP jitter test on known ports, namely, ports from 1 to 1023. Otherwise, the NQA test will fail or the corresponding services of this port will be unavailable.

Real-time services such as voice and video have high requirements on delay jitters. With the UDP jitter test, uni/bi-directional delay jitters can be obtained to judge whether a network can carry real-time services.

Delay jitter refers to the difference between the interval of receiving two packets consecutively and the interval of sending these two packets. The procedure of a UDP jitter test is as follows:

- The source sends packets at regular intervals to the destination port.
- The destination affixes a time stamp to each packet that it receives and then sends it back to the source.
- Upon receiving the packet, the source calculates the delay jitter, and the network status can be analyzed.

### Configuration prerequisites

A UDP jitter test requires cooperation between the NQA server and the NQA client. Before the UDP jitter test, make sure that the UDP listening function is configured on the NQA server. For the configuration of the UDP listening function, see Configuring the NQA Server.

### Configuring a UDP jitter test

Follow these steps to configure a UDP jitter test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as UDP jitter and enter test type view | **type udp-jitter** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination IP address must be consistent with that of the existing listening service on the NQA server. |
| Configure the destination port for a test operation | **destination port** *port-number* | Required<br>By default, no destination port number is configured for a test operation.<br>The destination port must be consistent with that of the existing listening service on the NQA server. |
| Specify the source port number for a request | **source port** *port-number* | Optional<br>By default, no source port number is specified. |
| Configure the size of a probe packet sent | **data-size** *size* | Optional<br>100 bytes by default. |
| Configure the filler string of a probe packet sent | **data-fill** *string* | Optional<br>By default, the filler string of a probe packet is the hexadecimal number 00010203040506070809. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the number of packets sent in a UDP jitter probe | **probe packet-number** *packet-number* | Optional<br>10 by default. |
| Configure the interval for sending packets in a UDP jitter probe | **probe packet-interval** *packet-interval* | Optional<br>20 milliseconds by default. |
| Configure the time for waiting for a response in a UDP jitter test | **probe packet-timeout** *packet-timeout* | Optional<br>3000 milliseconds by default. |
| Configure the source IP address of a probe request in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

**Note**

The number of probes made in a UDP jitter test depends on the **probe count** command, while the number of probe packets sent in each probe depends on the configuration of the **probe packet-number** command.

## Configuring an SNMP Test

An SNMP query test is used to test the time the NQA client takes to send an SNMP query packet to the SNMP agent and then receive a response packet.

### Configuration prerequisites

The SNMP agent function must be enabled on the device serving as an SNMP agent before an SNMP test. For the configuration of SNMP agent, see *SNMP Configuration* in the *System Volume*.

### Configuring an SNMP test

Follow these steps to configure an SNMP test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as SNMP and enter test type view | **type snmp** | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation. |
| Specify the source port number for a probe request in a test operation | **source port** *port-number* | Optional<br>By default, no source port number is specified. |
| Configure the source IP address of a probe request in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

## Configuring a TCP Test

A TCP test is used to test the TCP connection between the client and the specified port on the NQA server and the setup time for the connection, thus judge the availability and performance of the services provided on the specified port on the server.

### Configuration prerequisites

A TCP test requires cooperation between the NQA server and the NQA client. The TCP listening function needs to be configured on the NQA server before the TCP test. For the configuration of the TCP listening function, see Configuring the NQA Server.

### Configuring a TCP test

Follow these steps to configure a TCP test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as TCP and enter test type view | **type tcp** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination address must be the IP address of the listening service configured on the NQA server. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination port | **destination port** *port-number* | Required<br>By default, no destination port number is configured for a test operation.<br>The destination port number must be consistent with port number of the listening service configured on the NQA server. |
| Configure the source IP address of a probe request in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

## Configuring a UDP Echo Test

A UDP echo test is used to test the connectivity and roundtrip time of a UDP echo packet from the client to the specified UDP port on the NQA server.

### Configuration prerequisites

A UDP echo test requires cooperation between the NQA server and the NQA client. The UDP listening function needs to be configured on the NQA server before the UDP echo test. For the configuration of the UDP listening function, see Configuring the NQA Server.

### Configuring a UDP echo test

Follow these steps to configure a UDP echo test

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as UDP echo and enter test type view | **type udp-echo** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination address must be the IP address of the listening service configured on the NQA server. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination port | **destination port** *port-number* | Required<br>By default, no destination port number is configured for a test operation.<br>The destination port number must be the port number of the listening service configured on the NQA server. |
| Configure the size of probe packets sent | **data-size** *size* | Optional<br>100 bytes by default. |
| Configure the filler string of a probe packet sent | **data-fill** *string* | Optional<br>By default, the filler string of a probe packet is the hexadecimal number 00010203040506070809. |
| Specify a source port number for a probe request in a test operation | **source port** *port-number* | Optional<br>By default, no source port number is specified. |
| Configure the source IP address of a probe request in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

## Configuring a Voice Test

**Note**

It is recommended not to perform an NQA UDP jitter test on known ports, namely, ports from 1 to 1023. Otherwise, the NQA test will fail or the corresponding services of these ports will be unavailable.

A voice test is used to test voice over IP (VoIP) network status, and collect VoIP network parameters so that users can adjust the network according the network status. The procedure of a voice test is as follows:

1) The source (NQA client) sends voice packets of G.711 A-law, G.711 μ-law or G.729 A-law codec type at regular intervals to the destination (NQA server).
2) The destination affixes a time stamp to each packet that it receives and then sends it back to the source.
3) Upon receiving the packets, the source calculates the delay jitter and delay by calculating the difference between the interval for the destination to receive two successive packets and the

interval for the source to send these two successive packets, and thus the network status can be analyzed.

The voice parameter values that indicate VoIP network status can also be calculated in a voice test, including:

- Calculated Planning Impairment Factor (ICPIF): Measures attenuation of voice data in a network, depending on packet loss and delay. A higher value represents a lower network quality.
- Mean Opinion Scores (MOS): Measures quality of a VoIP network. A MOS value can be evaluated by using the ICPIF value, in the range 1 to 15. A higher value represents a higher quality of a VoIP network.

The evaluation of voice quality depends on users' tolerance to voice quality, and this factor should be taken into consideration. For users with higher tolerance to voice quality, you can use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values and thus both the objective and subjective factors are considered when you evaluate the voice quality.

### Configuration prerequisites

A voice test requires cooperation between the NQA server and the NQA client. Before a voice test, make sure that the UDP listening function is configured on the NQA server. For the configuration of UDP listening function, see Configuring the NQA Server.

### Configuring a voice test

Follow these steps to configure a voice test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as voice and enter test type view | **type voice** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation.<br>The destination IP address must be consistent with that of the existing listening service on the NQA server. |
| Configure the destination port for a test operation | **destination port** *port-number* | Required<br>By default, no destination port number is configured for a test operation.<br>The destination port must be consistent with that of the existing listening service on the NQA server. |
| Configure the codec type | **codec-type** { **g711a** \| **g711u** \| **g729a** } | Optional<br>By default, the codec type is G.711 A-law. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the advantage factor for calculating MOS and ICPIF values | **advantage-factor** *factor* | Optional<br>By default, the advantage factor is 0. |
| Specify the source IP address for the requests in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Specify the source port number for the requests in a test operation | **source port** *port-number* | Optional<br>By default, no source port number is specified. |
| Configure the size of a probe packet to be sent | **data-size** *size* | Optional<br>By default, the probe packet size depends on the codec type. The default packet size is 172 bytes for G.711A-law and G.711 μ-law codec type, and is 32 bytes for G.729 A-law codec type. |
| Configure the filler string of a probe packet sent | **data-fill** *string* | Optional<br>By default, the filler string of a probe packet is the hexadecimal number 00010203040506070809. |
| Configure the number of packets sent in a voice probe | **probe packet-number** *packet-number* | Optional<br>1000 by default. |
| Configure the interval for sending packets in a voice probe | **probe packet-interval** *packet-interval* | Optional<br>20 milliseconds by default. |
| Configure the timeout for waiting for a response in a voice test | **probe packet-timeout** *packet-timeout* | Optional<br>5000 milliseconds by default. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

**Note**

Only one probe can be made in one voice test, and the number of probe packets sent in each probe depends on the configuration of the **probe packet-number** command.

## Configuring a DLSw Test

A DLSw test is used to test the response time of the DLSw device.

### Configuration prerequisites

Enable the DLSw function on the peer device before DLSw test.

### Configuring a DLSw test

Follow these steps to configure a DLSw test:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Configure the test type as DLSw and enter test type view | **type dlsw** | Required |
| Configure the destination address for a test operation | **destination ip** *ip-address* | Required<br>By default, no destination IP address is configured for a test operation. |
| Configure the source IP address of a probe request in a test operation | **source ip** *ip-address* | Optional<br>By default, no source IP address is specified.<br>The source IP address must be that of an interface on the device and the interface must be up. Otherwise, the test will fail. |
| Configure common optional parameters | See Configuring Optional Parameters Common to an NQA Test Group | Optional |

## Configuring the Collaboration Function

Collaboration is implemented by establishing collaboration objects to monitor the detection results of the current test group. If the number of consecutive probe failures reaches the threshold, the configured action is triggered.

Follow these steps to configure the collaboration function:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Enter test type view of the test group | **type** { **dhcp** \| **dlsw** \| **ftp** \| **http** \| **icmp-echo** \| **snmp** \| **tcp** \| **udp-echo** } | The collaboration function is not supported in UDP jitter or voice tests. |
| Create a collaboration object | **reaction** *item-num* **checked-element probe-fail threshold-type consecutive** *occurrences* [ **action-type** { **none** \| **trigger-only** } ] | Required<br>Not created by default. |
| Exit to system view | **quit** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a Track object and associate it with the specified collaboration object of the NQA test group | **track** *entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-num* | Required<br>Not created by default. |

**Note**

- You cannot modify the content of a reaction entry using the **reaction** command after the collaboration object is created.
- The collaboration function is not supported in a UDP jitter or voice test.

# Configuring Trap Delivery

Traps can be sent to the network management server when test is completed, test fails or probe fails.

## Configuration prerequisites

Before configuring trap delivery, you need to configure the destination address of the trap message with the **snmp-agent target-host** command, create an NQA test group, and configure related parameters. For the introduction to the **snmp-agent target-host** command, see *SNMP Commands* in the *System Volume*.

## Configuring trap delivery

Follow these steps to configure trap delivery:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Enter test type view of the test group | **type** { **dhcp** \| **dlsw** \| **ftp** \| **http** \| **icmp-echo** \| **snmp** \| **tcp** \| **udp-echo** \| **udp-jitter** \| **voice** } | — |
| Configure to send traps to network management server under specified conditions | **reaction trap** { **probe-failure** *consecutive-probe-failures* \| **test-complete** \| **test-failure** *cumulate-probe-failures* } | Optional<br>No traps are sent to the network management server by default. |

**Note**

Only the **reaction trap test-complete** command is supported in a voice test, namely, in a voice test, traps are sent to the NMS only if the test succeeds.

## Configuring the NQA Statistics Function

NQA puts the NQA tests completed in a specified interval into one group, and calculates the statistics of the test results of the group. These statistics form a statistics group. You can use the **display nqa statistics** command to view information of the statistics group, and use the **statistics interval** command to set the interval for collecting statistics.

When the number of statistics groups kept reaches the upper limit, if a new statistics group is generated, the statistics group that is kept for the longest time is deleted. You can use the **statistics max-group** command to set the maximum number of statistics groups that can be kept.

A statistics group is formed after the last test is completed within the specified interval. A statistics group has the aging mechanism. A statistics group will be deleted after it is kept for a period of time. You can use the **statistics hold-time** command to set the hold time of a statistics group.

Follow these steps to configure the NQA statistics function:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Enter test type view of the test group | **type** { **dlsw** \| **ftp** \| **http** \| **icmp-echo** \| **snmp** \| **tcp** \| **udp-echo** \| **udp-jitter** \| **voice** } | — |
| Configure the interval for collecting the statistics of the test results | **statistics interval** *interval* | Optional<br>60 minutes by default. |
| Configure the maximum number of statistics groups that can be kept | **statistics max-group** *number* | Optional<br>2 by default.<br>If the maximum number is 0, it indicates that no statistics is performed. |
| Configure the hold time of a statistics group | **statistics hold-time** *hold-time* | Optional<br>120 minutes by default. |

**Note**

- The NQA statistics function is not supported in a DHCP test.
- If you specify the *interval* argument in the **frequency** *interval* command as 0, no statistics group information is generated.

## Configuring Optional Parameters Common to an NQA Test Group

Optional parameters common to an NQA test group are valid only for tests in this test group.

Unless otherwise specified, the following parameters are applicable to all test types and they can be configured according to the actual conditions.

Follow these steps to configure optional parameters common to an NQA test group:

| To do… | Use the command… | Remarks |
| --- | --- | --- |
| Enter system view | **system-view** | — |
| Enter NQA test group view | **nqa entry** *admin-name operation-tag* | — |
| Enter test type view of a test group | **type** { **dhcp** \| **dlsw** \| **ftp** \| **http** \| **icmp-echo** \| **snmp** \| **tcp** \| **udp-echo** \| **udp-jitter** \| **voice** } | — |
| Configure the descriptive string for a test group | **description** *text* | Optional<br>By default, no descriptive string is available for a test group. |
| Configure the interval between two consecutive tests for a test group | **frequency** *interval* | Optional<br>By default, the interval between two consecutive tests for a test group is 0 milliseconds, that is, only one test is performed.<br>If the last test is not completed when the interval specified by the **frequency** command is reached, a new test is not started. |
| Configure the number of probes in an NQA test | **probe count** *times* | Optional<br>By default, one probe is performed in a test.<br>Only one probe can be made in one voice test. Therefore, this command is not available in a voice test. |
| Configure the NQA probe timeout time | **probe timeout** *timeout* | Optional<br>By default, the timeout time is 3000 milliseconds.<br>This parameter is not available for a UDP jitter test. |
| Configure the maximum number of history records that can be saved in a test group | **history-records** *number* | Optional<br>50 by default. |
| Configure the maximum number of hops a probe packet traverses in the network | **ttl** *value* | Optional<br>20 by default.<br>This parameter is not available for a DHCP test. |
| Configure the ToS field in an IP packet header in an NQA probe packet | **tos** *value* | Optional<br>0 by default.<br>This parameter is not available for a DHCP test. |
| Enable the routing table bypass function | **route-option bypass-route** | Optional<br>Disabled by default.<br>This parameter is not available for a DHCP test. |

# Scheduling an NQA Test Group

With this configuration, you can set the start time and test duration for a test group to perform NQA tests. The start time can take a specific value or can be **now**, which indicates that a test is started immediately; the test duration can take a specific value or can be **forever**, which indicates that a test will not stop until you use the **undo nqa schedule** command to stop the test.

A test group performs tests when the system time is between the start time and the end time (the start time plus test duration). If the system time is behind the start time when you execute the **nqa schedule** command, a test is started when the system time reaches the start time; if the system time is between the start time and the end time, a test is started at once; if the system time is ahead of the end time, no test is started. You can use the **display clock** command to view the current system time.

## Configuration prerequisites

Before scheduling an NQA test group, make sure:

- Required test parameters corresponding to a test type have been configured;
- For the test which needs the cooperation with the NQA server, configuration on the NQA server has been completed.

## Scheduling an NQA test group

Follow these steps to schedule an NQA test group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Schedule an NQA test group | **nqa schedule** *admin-name operation-tag* **start-time** { *hh:mm:ss* [ *yyyy/mm/dd* ] \| **now** } **lifetime** { *lifetime* \| **forever** } | Required |
| Configure the maximum number of the tests that the NQA client can simultaneously perform | **nqa agent max-concurrent** *number* | Optional<br>2 by default. |

**Caution**

- After an NQA test group is scheduled, you cannot enter the test group view or test type view.
- A started test group or a test group that has completed tests will not be influenced by the system time change; only a test group that is waiting to perform tests will be influenced by the system time change.

# Displaying and Maintaining NQA

| To do… | Use the command… | Remarks |
|---|---|---|
| Display history records of NQA test operation information | **display nqa history** [ *admin-name operation-tag* ] | Available in any view |
| Display the results of the last NQA test | **display nqa result** [ *admin-name operation-tag* ] | |
| Display the statistics of a type of NQA test | **display nqa statistics** [ *admin-name operation-tag* ] | |
| Display NQA server status | **display nqa server status** | |

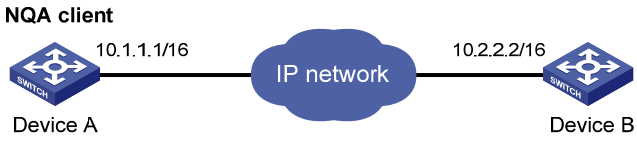
# NQA Configuration Examples

## ICMP Echo Test Configuration Example

### Network requirements

Use the NQA ICMP function to test whether the NQA client (Device A) can send packets to the specified destination (Device B) and test the roundtrip time of packets.

**Figure 1-3** Network diagram for ICMP echo tests




### Configuration procedure

# Create an ICMP echo test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type icmp-echo
[DeviceA-nqa-admin-test-icmp-echo] destination ip 10.2.2.2
```

# Configure optional parameters.

```
[DeviceA-nqa-admin-test-icmp-echo] probe count 10
[DeviceA-nqa-admin-test-icmp-echo] probe timeout 500
[DeviceA-nqa-admin-test-icmp-echo] frequency 5000
[DeviceA-nqa-admin-test-icmp-echo] history-records 10
[DeviceA-nqa-admin-test-icmp-echo] quit
```

# Enable ICMP echo test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable ICMP echo test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last ICMP echo test.

```
[DeviceA] display nqa result admin test
```

```
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average round trip time: 2/5/3
      Square-Sum of round trip time: 96
      Last succeeded probe time: 2007-08-23 15:00:01.2
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of ICMP echo tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    370        3            Succeeded        2007-08-23 15:00:01.2
    369        3            Succeeded        2007-08-23 15:00:01.2
    368        3            Succeeded        2007-08-23 15:00:01.2
    367        5            Succeeded        2007-08-23 15:00:01.2
    366        3            Succeeded        2007-08-23 15:00:01.2
    365        3            Succeeded        2007-08-23 15:00:01.2
    364        3            Succeeded        2007-08-23 15:00:01.1
    363        2            Succeeded        2007-08-23 15:00:01.1
    362        3            Succeeded        2007-08-23 15:00:01.1
    361        2            Succeeded        2007-08-23 15:00:01.1
```

## DHCP Test Configuration Example

### Network requirements

Use the NQA DHCP function to test the time necessary for Switch A to obtain an IP address from the DHCP server Switch B.

**Figure 1-4** Network diagram for DHCP


### Configuration procedure

# Create a DHCP test group and configure related test parameters.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
```

```
[SwitchA-nqa-admin-test] type dhcp
[SwitchA-nqa-admin-test-dhcp] operation interface vlan-interface 2
[SwitchA-nqa-admin-test-dhcp] quit
```

# Enable DHCP test.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# Disable DHCP test after the test begins for a period of time.

```
[SwitchA] undo nqa schedule admin test
```

# Display the result of the last DHCP test.

```
[SwitchA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 624/624/624
      Square-Sum of round trip time: 389376
      Last succeeded probe time: 2007-11-22 09:56:03.2
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of DHCP tests.

```
[SwitchA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          624          Succeeded        2007-11-22 09:56:03.2
```

## FTP Test Configuration Example

### Network requirements

Use the NQA FTP function to test the connection with a specified FTP server and the time necessary for Device A to upload a file to the FTP server. The login username is **admin**, the login password is **systemtest**, and the file to be transferred to the FTP server is **config.txt**.

**Figure 1-5** Network diagram for FTP tests


### Configuration procedure

# Create an FTP test group and configure related test parameters.

```
<DeviceA> system-view
```

```
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type ftp
[DeviceA-nqa-admin-test-ftp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-ftp] source ip 10.1.1.1
[DeviceA-nqa-admin-test-ftp] operation put
[DeviceA-nqa-admin-test-ftp] username admin
[DeviceA-nqa-admin-test-ftp] password systemtest
[DeviceA-nqa-admin-test-ftp] filename config.txt
[DeviceA-nqa-admin-test-ftp] quit
```

# Enable FTP test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable FTP test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last FTP test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 173/173/173
      Square-Sum of round trip time: 29929
      Last succeeded probe time: 2007-11-22 10:07:28.6
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of FTP tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          173          Succeeded        2007-11-22 10:07:28.6
```

## HTTP Test Configuration Example

### Network requirements

Use the HTTP function to test the connection with a specified HTTP server and the time required to obtain data from the HTTP server.

**Figure 1-6** Network diagram for the HTTP tests


## Configuration procedure

# Create an HTTP test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type http
[DeviceA-nqa-admin-test-http] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-http] operation get
[DeviceA-nqa-admin-test-http] url /index.htm
[DeviceA-nqa-admin-test-http] http-version v1.0
[DeviceA-nqa-admin-test-http] quit
```

# Enable HTTP test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable HTTP test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last HTTP test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 64/64/64
      Square-Sum of round trip time: 4096
      Last succeeded probe time: 2007-11-22 10:12:47.9
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors:
      Packet(s) arrived late: 0
```

# Display the history of HTTP tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          64           Succeeded        2007-11-22 10:12:47.9
```

## UDP Jitter Test Configuration Example

### Network requirements

Use the NQA UDP jitter function to test the delay jitter of packet transmission between Device A and Device B.

**Figure 1-7** Network diagram for UDP jitter tests


### Configuration procedure

1) Configure Device B.

# Enable the NQA server and configure the listening IP address as 10.2.2.2 and port number as 9000.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

2) Configure Device A.

# Create a UDP jitter test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-jitter
[DeviceA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-jitter] destination port 9000
[DeviceA-nqa-admin-test-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test-udp-jitter] quit
```

# Enable UDP jitter test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable UDP jitter test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display the result of the last UDP jitter test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average round trip time: 15/32/17
      Square-Sum of round trip time: 3235
      Last succeeded probe time: 2008-05-29 13:56:17.6
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
```

```
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packet(s) arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 4                    Min positive DS: 1
    Max positive SD: 21                   Max positive DS: 28
    Positive SD number: 5                 Positive DS number: 4
    Positive SD sum: 52                   Positive DS sum: 38
    Positive SD average: 10               Positive DS average: 10
    Positive SD square sum: 754           Positive DS square sum: 460
    Min negative SD: 1                    Min negative DS: 6
    Max negative SD: 13                   Max negative DS: 22
    Negative SD number: 4                 Negative DS number: 5
    Negative SD sum: 38                   Negative DS sum: 52
    Negative SD average: 10               Negative DS average: 10
    Negative SD square sum: 460           Negative DS square sum: 754
  One way results:
    Max SD delay: 15                      Max DS delay: 16
    Min SD delay: 7                       Min DS delay: 7
    Number of SD delay: 10                Number of DS delay: 10
    Sum of SD delay: 78                   Sum of DS delay: 85
    Square sum of SD delay: 666           Square sum of DS delay: 787
    SD lost packet(s): 0                  DS lost packet(s): 0
    Lost packet(s) for unknown reason: 0
```

# Display the statistics of UDP jitter tests.

```
[DeviceA] display nqa statistics admin test
  NQA entry(admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 10.2.2.2
      Start time: 2008-05-29 13:56:14.0
      Life time: 47
      Send operation times: 410           Receive response times: 410
      Min/Max/Average round trip time: 1/93/19
      Square-Sum of round trip time: 206176
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 410
```

```
  Min positive SD: 3                  Min positive DS: 1
  Max positive SD: 30                 Max positive DS: 79
  Positive SD number: 186             Positive DS number: 158
  Positive SD sum: 2602               Positive DS sum: 1928
  Positive SD average: 13             Positive DS average: 12
  Positive SD square sum: 45304       Positive DS square sum: 31682
  Min negative SD: 1                  Min negative DS: 1
  Max negative SD: 30                 Max negative DS: 78
  Negative SD number: 181             Negative DS number: 209
  Negative SD sum: 181                Negative DS sum: 209
  Negative SD average: 13             Negative DS average: 14
  Negative SD square sum: 46994       Negative DS square sum: 3030
One way results:
  Max SD delay: 46                    Max DS delay: 46
  Min SD delay: 7                     Min DS delay: 7
  Number of SD delay: 410             Number of DS delay: 410
  Sum of SD delay: 3705               Sum of DS delay: 3891
  Square sum of SD delay: 45987       Square sum of DS delay: 49393
  SD lost packet(s): 0                DS lost packet(s): 0
  Lost packet(s) for unknown reason: 0
```

**Note**

The **display nqa history** command cannot show you the results of UDP jitter tests. Therefore, to know the result of a UDP jitter test, you are recommended to use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

## SNMP Test Configuration Example

### Network requirements

Use the NQA SNMP query function to test the time it takes for Device A to send an SNMP query packet to the SNMP agent and receive a response packet.

**Figure 1-8** Network diagram for SNMP tests


### Configuration procedure

1) Configurations on SNMP agent.

# Enable the SNMP agent service and set the SNMP version to **all**, the read community to **public**, and the write community to **private**.

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
```

2) Configurations on Device A.

# Create an SNMP query test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type snmp
[DeviceA-nqa-admin-test-snmp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-snmp] quit
```

# Enable SNMP query test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable SNMP query test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last SNMP test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 50/50/50
      Square-Sum of round trip time: 2500
      Last succeeded probe time: 2007-11-22 10:24:41.1
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of SNMP tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          50           Timeout          2007-11-22 10:24:41.1
```

## TCP Test Configuration Example

### Network requirements

Use the NQA TCP function to test the time for establishing a TCP connection between Device A and Device B. The port number used is 9000.

**Figure 1-9** Network diagram for TCP tests


## Configuration procedure

1) Configure Device B.

# Enable the NQA server and configure the listening IP address as 10.2.2.2 and port number as 9000.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

2) Configure Device A.

# Create a TCP test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type tcp
[DeviceA-nqa-admin-test-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-tcp] destination port 9000
[DeviceA-nqa-admin-test-tcp] quit
```

# Enable TCP test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable TCP test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last TCP test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 13/13/13
      Square-Sum of round trip time: 169
      Last succeeded probe time: 2007-11-22 10:27:25.1
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of TCP tests.

```
[DeviceA] display nqa history admin test
```

```
NQA entry(admin admin, tag test) history record(s):
  Index      Response     Status           Time
  1          13           Succeeded        2007-11-22 10:27:25.1
```

## UDP Echo Test Configuration Example

### Network requirements

Use the NQA UDP echo function to test the round trip time between Device A and Device B. The port number is 8000.

**Figure 1-10** Network diagram for the UDP echo tests


### Configuration procedure

1) Configure Device B.

# Enable the NQA server and configure the listening IP address as 10.2.2.2 and port number as 8000.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

2) Configure Device A.

# Create a UDP echo test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-echo
[DeviceA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-echo] destination port 8000
[DeviceA-nqa-admin-test-udp-echo] quit
```

# Enable UDP echo test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable UDP echo test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display results of the last UDP echo test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 25/25/25
      Square-Sum of round trip time: 625
      Last succeeded probe time: 2007-11-22 10:36:17.9
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
```

```
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packet(s) arrived late: 0
```

# Display the history of UDP echo tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          25           Succeeded        2007-11-22 10:36:17.9
```

## Voice Test Configuration Example

### Network requirements

Use the NQA voice function to test the delay jitter of voice packet transmission and voice quality between Device A and Device B.

**Figure 1-11** Network diagram for voice tests


### Configuration procedure

1) Configure Device B.

# Enable the NQA server and configure the listening IP address as 10.2.2.2 and port number as 9000.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

2) Configure Device A.

# Create a voice test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type voice
[DeviceA-nqa-admin-test-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-voice] destination port 9000
[DeviceA-nqa-admin-test-voice] quit
```

# Enable voice test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable the voice test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display the result of the last voice test.

```
[DeviceA] display nqa result admin test
```

```
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1000           Receive response times: 1000
      Min/Max/Average round trip time: 31/1328/33
      Square-Sum of round trip time: 2844813
      Last succeeded probe time: 2008-06-13 09:49:31.1
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 1000
      Min positive SD: 1                   Min positive DS: 1
      Max positive SD: 204                 Max positive DS: 1297
      Positive SD number: 257              Positive DS number: 259
      Positive SD sum: 759                 Positive DS sum: 1797
      Positive SD average: 2               Positive DS average: 6
      Positive SD square sum: 54127        Positive DS square sum: 1691967
      Min negative SD: 1                   Min negative DS: 1
      Max negative SD: 203                 Max negative DS: 1297
      Negative SD number: 255              Negative DS number: 259
      Negative SD sum: 759                 Negative DS sum: 1796
      Negative SD average: 2               Negative DS average: 6
      Negative SD square sum: 53655        Negative DS square sum: 1691776
    One way results:
      Max SD delay: 343                    Max DS delay: 985
      Min SD delay: 343                    Min DS delay: 985
      Number of SD delay: 1                Number of DS delay: 1
      Sum of SD delay: 343                 Sum of DS delay: 985
      Square sum of SD delay: 117649       Square sum of DS delay: 970225
      SD lost packet(s): 0                 DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
    Voice scores:
      MOS value: 4.38                      ICPIF value: 0
```

# Display the statistics of voice tests.

```
[DeviceA] display nqa statistics admin test
  NQA entry(admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 10.2.2.2
      Start time: 2008-06-13 09:45:37.8
      Life time: 331
      Send operation times: 4000           Receive response times: 4000
```

```
  Min/Max/Average round trip time: 15/1328/32
  Square-Sum of round trip time: 7160528
Extended results:
  Packet lost in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
Voice results:
 RTT number: 4000
  Min positive SD: 1                    Min positive DS: 1
  Max positive SD: 360                  Max positive DS: 1297
  Positive SD number: 1030              Positive DS number: 1024
  Positive SD sum: 4363                 Positive DS sum: 5423
  Positive SD average: 4                Positive DS average: 5
  Positive SD square sum: 497725        Positive DS square sum: 2254957
  Min negative SD: 1                    Min negative DS: 1
  Max negative SD: 360                  Max negative DS: 1297
  Negative SD number: 1028              Negative DS number: 1022
  Negative SD sum: 1028                 Negative DS sum: 1022
  Negative SD average: 4                Negative DS average: 5
  Negative SD square sum: 495901        Negative DS square sum: 5419
One way results:
  Max SD delay: 359                     Max DS delay: 985
  Min SD delay: 0                       Min DS delay: 0
  Number of SD delay: 4                 Number of DS delay: 4
  Sum of SD delay: 1390                 Sum of DS delay: 1079
  Square sum of SD delay: 483202        Square sum of DS delay: 973651
  SD lost packet(s): 0                  DS lost packet(s): 0
  Lost packet(s) for unknown reason: 0
Voice scores:
  Max MOS value: 4.38                   Min MOS value: 4.38
  Max ICPIF value: 0                    Min ICPIF value: 0
```

**Note**

The **display nqa history** command cannot show you the results of voice tests. Therefore, to know the result of a voice test, you are recommended to use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

## DLSw Test Configuration Example

### Network requirements

Use the NQA DLSw function to test the response time of the DLSw device.

**Figure 1-12** Network diagram for the DLSw tests


### Configuration procedure

# Create a DLSw test group and configure related test parameters.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dlsw
[DeviceA-nqa-admin-test-dlsw] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-dlsw] quit
```

# Enable DLSw test.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# Disable DLSw test after the test begins for a period of time.

```
[DeviceA] undo nqa schedule admin test
```

# Display the result of the last DLSw test.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 19/19/19
      Square-Sum of round trip time: 361
      Last succeeded probe time: 2007-11-22 10:40:27.7
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

# Display the history of DLSw tests.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          19           Succeeded        2007-11-22 10:40:27.7
```

# Table of Contents

# 1 NTP Configuration

When configuring NTP, go to these sections for information you are interested in:



## NTP Overview

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP runs over the User Datagram Protocol (UDP), using UDP port 123.

The purpose of using NTP is to keep consistent timekeeping among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time.

For a local system running NTP, its time can be synchronized by other reference sources and can be used as a reference source to synchronize other clocks.

### Applications of NTP

An administrator can by no means keep time synchronized among all the devices within a network by changing the system clock on each station, because this is a huge amount of workload and cannot guarantee the clock precision. NTP, however, allows quick clock synchronization within the entire network while it ensures a high clock precision.

NTP is used when all devices within the network must be consistent in timekeeping, for example:

- In analysis of the log information and debugging information collected from different devices in network management, time must be used as reference basis.
- All devices must use the same reference clock in a charging system.
- To implement certain functions, such as scheduled restart of all devices within the network, all devices must be consistent in timekeeping.
- When multiple systems process a complex event in cooperation, these systems must use that same reference clock to ensure the correct execution sequence.
- For incremental backup between a backup server and clients, timekeeping must be synchronized between the backup server and all the clients.

### Advantages of NTP

- NTP uses a stratum to describe the clock precision, and is able to synchronize time among all devices within the network.
- NTP supports access control and MD5 authentication.

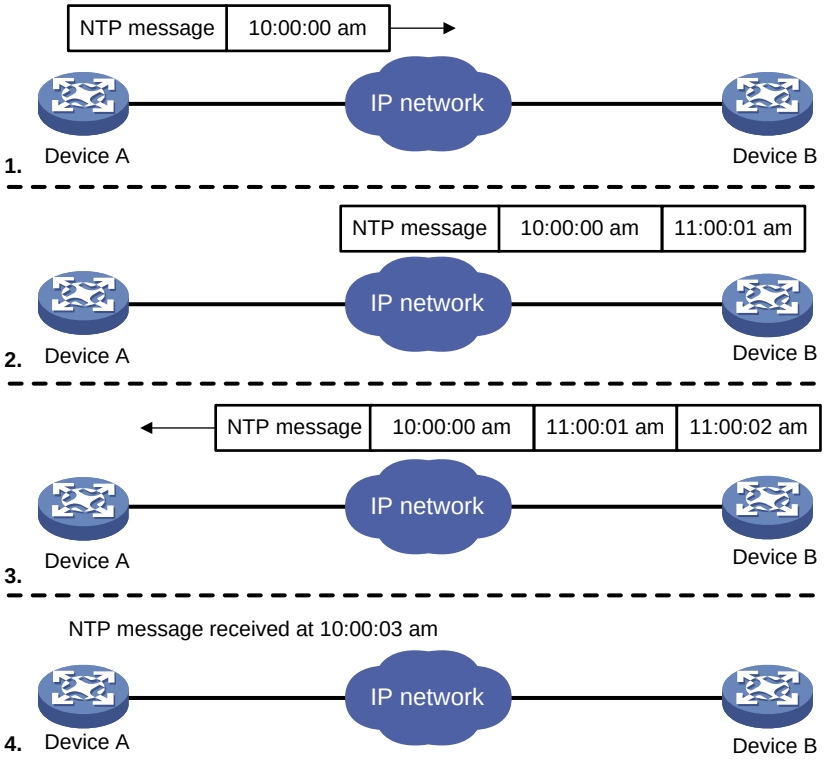
- NTP can unicast, multicast or broadcast protocol messages.

## How NTP Works

Figure 1-1 shows the basic workflow of NTP. Device A and Device B are interconnected over a network. They have their own independent system clocks, which need to be automatically synchronized through NTP. For an easy understanding, we assume that:

- Prior to system clock synchronization between Device A and Device B, the clock of Device A is set to 10:00:00 am while that of Device B is set to 11:00:00 am.
- Device B is used as the NTP time server, namely, Device A synchronizes its clock to that of Device B.
- It takes 1 second for an NTP message to travel from one device to the other.

**Figure 1-1** Basic work flow of NTP




The process of system clock synchronization is as follows:

- Device A sends Device B an NTP message, which is timestamped when it leaves Device A. The time stamp is 10:00:00 am (T1).
- When this NTP message arrives at Device B, it is timestamped by Device B. The timestamp is 11:00:01 am (T2).
- When the NTP message leaves Device B, Device B timestamps it. The timestamp is 11:00:02 am (T3).
- When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

Up to now, Device A has sufficient information to calculate the following two important parameters:

- The roundtrip delay of NTP message: Delay = (T4–T1) – (T3-T2) = 2 seconds.
- Time difference between Device A and Device B: Offset = ((T2-T1) + (T3-T4))/2 = 1 hour.

Based on these parameters, Device A can synchronize its own clock to the clock of Device B.

This is only a rough description of the work mechanism of NTP. For details, refer to RFC 1305.

## NTP Message Format

NTP uses two types of messages, clock synchronization message and NTP control message. An NTP control message is used in environments where network management is needed. As it is not a must for clock synchronization, it will not be discussed in this document.

---

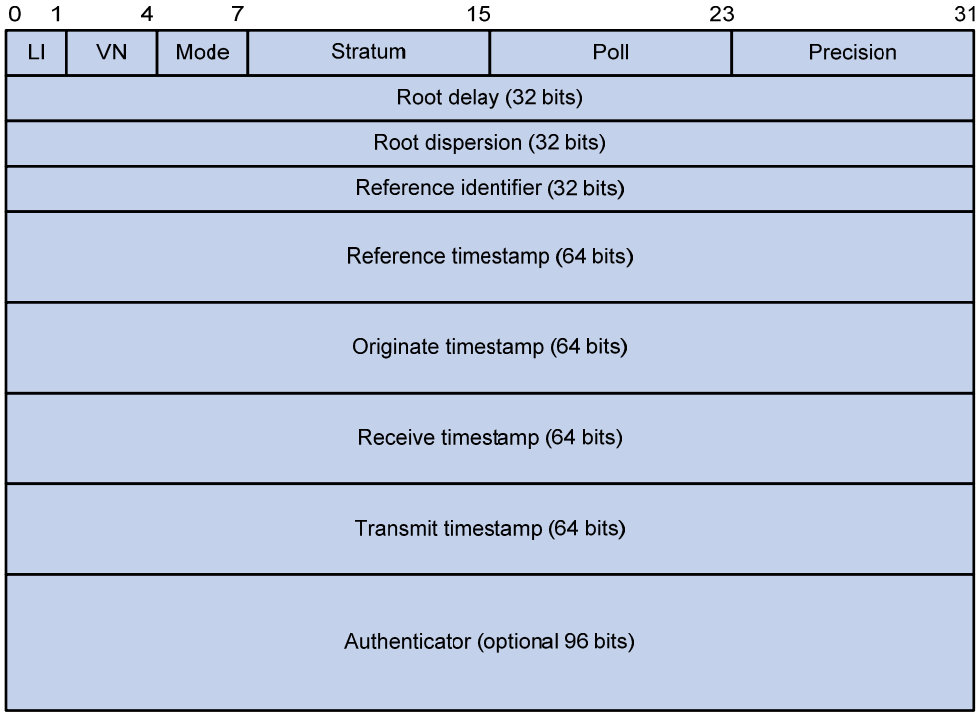
**Note**

All NTP messages mentioned in this document refer to NTP clock synchronization messages.

---

A clock synchronization message is encapsulated in a UDP message, in the format shown in Figure 1-2.

**Figure 1-2** Clock synchronization message format




Main fields are described as follows:

- LI: 2-bit leap indicator. When set to 11, it warns of an alarm condition (clock unsynchronized); when set to any other value, it is not to be processed by NTP.
- VN: 3-bit version number, indicating the version of NTP. The latest version is version 3.
- Mode: a 3-bit code indicating the work mode of NTP. This field can be set to these values: 0 – reserved; 1 – symmetric active; 2 – symmetric passive; 3 – client; 4 – server; 5 – broadcast or multicast; 6 – NTP control message; 7 – reserved for private use.
- Stratum: an 8-bit integer indicating the stratum level of the local clock, with the value ranging from 1 to 16. The clock precision decreases from stratum 1 through stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.

- Poll: 8-bit signed integer indicating the poll interval, namely the maximum interval between successive messages.
- Precision: an 8-bit signed integer indicating the precision of the local clock.
- Root Delay: roundtrip delay to the primary reference source.
- Root Dispersion: the maximum error of the local clock relative to the primary reference source.
- Reference Identifier: Identifier of the particular reference source.
- Reference Timestamp: the local time at which the local clock was last set or corrected.
- Originate Timestamp: the local time at which the request departed from the client for the service host.
- Receive Timestamp: the local time at which the request arrived at the service host.
- Transmit Timestamp: the local time at which the reply departed from the service host for the client.
- Authenticator: authentication information.

## Operation Modes of NTP

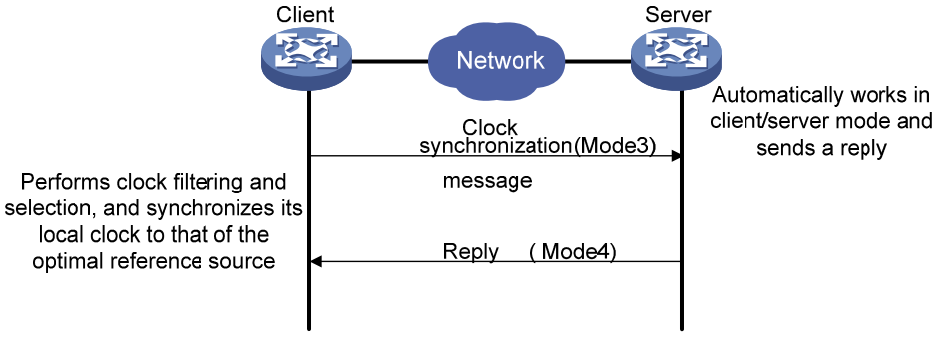
Devices running NTP can implement clock synchronization in one of the following modes:

- Client/server mode
- Symmetric peers mode
- Broadcast mode
- Multicast mode

You can select operation modes of NTP as needed. In case that the IP address of the NTP server or peer is unknown and many devices in the network need to be synchronized, you can adopt the broadcast or multicast mode; while in the client/server and symmetric peers modes, a device is synchronized from the specified server or peer, and thus clock reliability is enhanced.

### Client/server mode

**Figure 1-3** Client/server mode

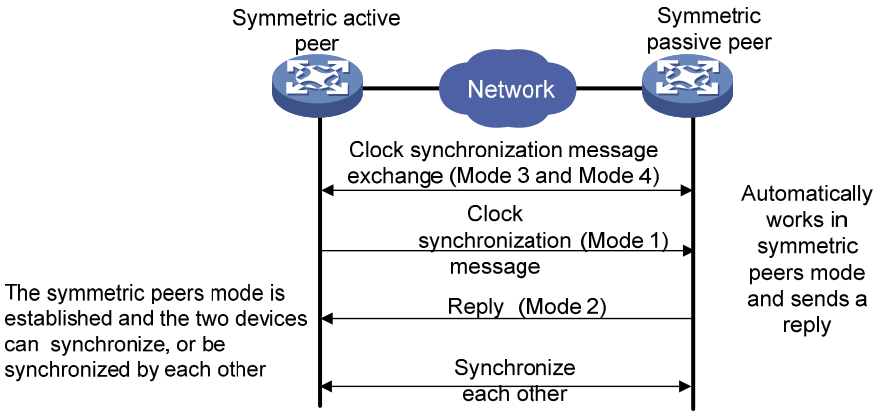



When working in the client/server mode, a client sends a clock synchronization message to servers, with the Mode field in the message set to 3 (client mode). Upon receiving the message, the servers automatically work in the server mode and send a reply, with the Mode field in the messages set to 4 (server mode). Upon receiving the replies from the servers, the client performs clock filtering and selection, and synchronizes its local clock to that of the optimal reference source.

In this mode, a client can be synchronized to a server, but not vice versa.

## Symmetric peers mode

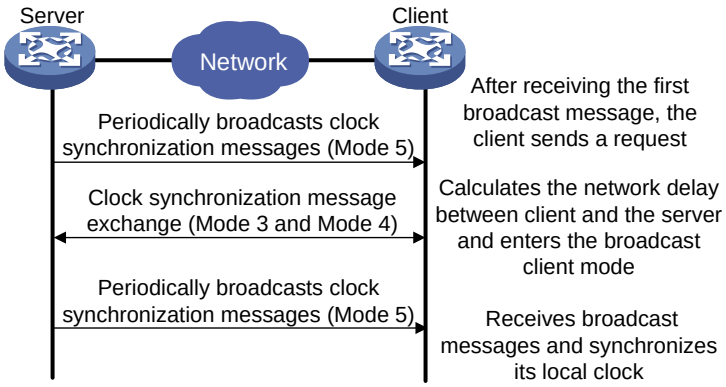
**Figure 1-4** Symmetric peers mode




A device working in the symmetric active mode periodically sends clock synchronization messages, with the Mode field in the message set to 1 (symmetric active); the device that receives this message automatically enters the symmetric passive mode and sends a reply, with the Mode field in the message set to 2 (symmetric passive). By exchanging messages, the symmetric peers mode is established between the two devices. Then, the two devices can synchronize, or be synchronized by each other. If the clocks of both devices have been already synchronized, the device whose local clock has a lower stratum level will synchronize the clock of the other device.

## Broadcast mode

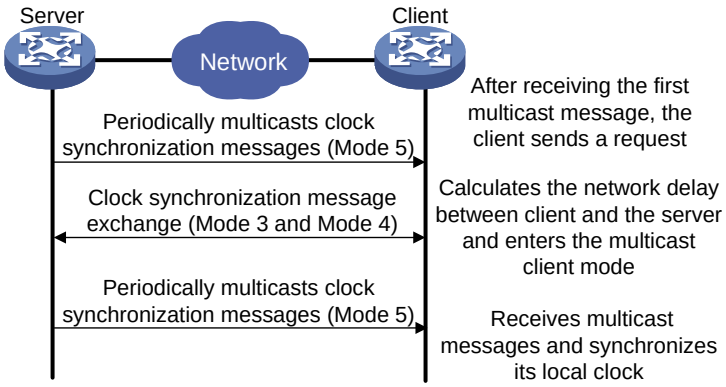
**Figure 1-5** Broadcast mode




In the broadcast mode, a server periodically sends clock synchronization messages to the broadcast address 255.255.255.255, with the Mode field in the messages set to 5 (broadcast mode). Clients listen to the broadcast messages from servers. After a client receives the first broadcast message, the client and the server start to exchange messages, with the Mode field set to 3 (client mode) and 4 (server mode) to calculate the network delay between client and the server. Then, the client enters the broadcast client mode and continues listening to broadcast messages, and synchronizes its local clock based on the received broadcast messages.

### Multicast mode

**Figure 1-6** Multicast mode




In the multicast mode, a server periodically sends clock synchronization messages to the user-configured multicast address, or, if no multicast address is configured, to the default NTP multicast address 224.0.1.1, with the Mode field in the messages set to 5 (multicast mode). Clients listen to the multicast messages from servers. After a client receives the first multicast message, the client and the server start to exchange messages, with the Mode field set to 3 (client mode) and 4 (server mode) to calculate the network delay between client and the server. Then, the client enters the multicast client mode and continues listening to multicast messages, and synchronizes its local clock based on the received multicast messages.

**Note**

In symmetric peers mode, broadcast mode and multicast mode, the client (or the symmetric active peer) and the server (the symmetric passive peer) can work in the specified NTP working mode only after they exchange NTP messages with the Mode field being 3 (client mode) and the Mode field being 4 (server mode). During this message exchange process, NTP clock synchronization can be implemented.

## NTP Configuration Task List

Complete the following tasks to configure NTP:

| Task | Remarks |
|---|---|
| Configuring the Operation Modes of NTP | Required |
| Configuring Optional Parameters of NTP | Optional |
| Configuring Access-Control Rights | Optional |
| Configuring NTP Authentication | Optional |

# Configuring the Operation Modes of NTP

Devices can implement clock synchronization in one of the following modes:

- Client/server mode
- Symmetric mode
- Broadcast mode
- Multicast mode

For the client/server mode or symmetric mode, you need to configure only clients or symmetric-active peers; for the broadcast or multicast mode, you need to configure both servers and clients.

---

**Note**

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time. In the client/server mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; in the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

---

## Configuring NTP Client/Server Mode

For devices working in the client/server mode, you only need to make configurations on the clients, but not on the servers.

Follow these steps to configure an NTP client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify an NTP server for the device | **ntp-service unicast-server** { *ip-address* \| *server-name* } [ **authentication-keyid** *keyid* \| **priority** \| **source-interface** *interface-type interface-number* \| **version** *number* ] * | Required<br>No NTP server is specified by default. |

**Note**

- In the **ntp-service unicast-server** command, *ip-address* must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.
- When the source interface for NTP messages is specified by the **source-interface** argument, the source IP address of the NTP messages will be configured as the primary IP address of the specified interface.
- A device can act as a server to synchronize the clock of other devices only after its clock has been synchronized. If the clock of a server has a stratum level higher than or equal to that of a client's clock, the client will not synchronize its clock to the server's.
- You can configure multiple servers by repeating the **ntp-service unicast-server** command. The clients will choose the optimal reference source.

## Configuring the NTP Symmetric Peers Mode

For devices working in the symmetric mode, you need to specify a symmetric-passive peer on a symmetric-active peer.

Following these steps to configure a symmetric-active device:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify a symmetric-passive peer for the device | **ntp-service unicast-peer** { *ip-address* \| *peer-name* } [ **authentication-keyid** *keyid* \| **priority** \| **source-interface** *interface-type interface-number* \| **version** *number* ] * | Required<br>No symmetric-passive peer is specified by default. |

**Note**

- In the symmetric mode, you should use any NTP configuration command in Configuring the Operation Modes of NTP to enable NTP; otherwise, a symmetric-passive peer will not process NTP messages from a symmetric-active peer.
- In the **ntp-service unicast-peer** command, *ip-address* must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.
- When the source interface for NTP messages is specified by the **source-interface** argument, the source IP address of the NTP messages will be configured as the primary IP address of the specified interface.
- Typically, at least one of the symmetric-active and symmetric-passive peers has been synchronized; otherwise the clock synchronization will not proceed.
- You can configure multiple symmetric-passive peers by repeating the **ntp-service unicast-peer** command.

## Configuring NTP Broadcast Mode

The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. After receiving the messages, the device working in NTP broadcast client mode sends a reply and synchronizes its local clock.

For devices working in the broadcast mode, you need to configure both the server and clients. Because an interface needs to be specified on the broadcast server for sending NTP broadcast messages and an interface also needs to be specified on each broadcast client for receiving broadcast messages, the NTP broadcast mode can be configured only in the specific interface view.

### Configuring a broadcast client

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Required<br>Enter the interface used to receive NTP broadcast messages. |
| Configure the device to work in the NTP broadcast client mode | **ntp-service broadcast-client** | Required |

### Configuring the broadcast server

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Enter the interface used to send NTP broadcast messages. |
| Configure the device to work in the NTP broadcast server mode | **ntp-service broadcast-server** [ **authentication-keyid** *keyid* \| **version** *number* ] * | Required |

**Note**

A broadcast server can synchronize broadcast clients only after its clock has been synchronized.

## Configuring NTP Multicast Mode

The multicast server periodically sends NTP multicast messages to multicast clients, which send replies after receiving the messages and synchronize their local clocks.

For devices working in the multicast mode, you need to configure both the server and clients. The NTP multicast mode must be configured in the specific interface view.

### Configuring a multicast client

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Enter the interface used to receive NTP multicast messages. |
| Configure the device to work in the NTP multicast client mode | **ntp-service multicast-client** [ *ip-address* ] | Required |

### Configuring the multicast server

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | Enter the interface used to send NTP multicast message. |
| Configure the device to work in the NTP multicast server mode | **ntp-service multicast-server** [ *ip-address* ] [ **authentication-keyid** *keyid* \| **ttl** *ttl-number* \| **version** *number* ] * | Required |

**Note**

- A multicast server can synchronize broadcast clients only after its clock has been synchronized.
- You can configure up to 1024 multicast clients, among which 128 can take effect at the same time.

# Configuring Optional Parameters of NTP

## Specifying the Source Interface for NTP Messages

If you specify the source interface for NTP messages, the device sets the source IP address of the NTP messages as the primary IP address of the specified interface when sending the NTP messages.

When the device responds to an NTP request received, the source IP address of the NTP response is always the IP address of the interface that received the NTP request.

Following these steps to specify the source interface for NTP messages:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify the source interface for NTP messages | **ntp-service source-interface** *interface-type interface-number* | Required<br>By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matching route as the source IP address of NTP messages. |

**Caution**

- If you have specified the source interface for NTP messages in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, the interface specified in the **ntp-service unicast-server** or **ntp-service unicast-peer** command serves as the source interface of NTP messages.
- If you have configured the **ntp-service broadcast-server** or **ntp-service multicast-server** command, the source interface of the broadcast or multicast NTP messages is the interface configured with the respective command.

## Disabling an Interface from Receiving NTP Messages

When NTP is enabled, NTP messages can be received from all the interfaces by default, and you can disable an interface from receiving NTP messages through the following configuration.

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Disable the interface from receiving NTP messages | **ntp-service in-interface disable** | Required<br>An interface is enabled to receive NTP messages by default. |

## Configuring the Maximum Number of Dynamic Sessions Allowed

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the maximum number of dynamic sessions allowed to be established locally | **ntp-service max-dynamic-sessions** *number* | Required<br>100 by default |

# Configuring Access-Control Rights

With the following command, you can configure the NTP service access-control right to the local device. There are four access-control rights, as follows:

- **query**: control query permitted. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device. The so-called “control query” refers to query of some states of the NTP service, including alarm information, authentication status, clock source information, and so on.
- **synchronization**: server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.
- **server**: server access and query permitted. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.
- **peer**: full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match and will use the first matched right.

## Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local device, you need to create and configure an ACL associated with the access-control right. For the configuration of ACL, refer to *ACL Configuration* in the *Security Volume*.

## Configuration Procedure

Follow these steps to configure the NTP service access-control right to the local device:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the NTP service access-control right for a peer device to access the local device | **ntp-service access** { **peer** \| **query** \| **server** \| **synchronization** } *acl-number* | Required<br>**peer** by default |

**Note**

The access-control right mechanism provides only a minimum degree of security protection for the system running NTP. A more secure method is identity authentication.

# Configuring NTP Authentication

The NTP authentication feature should be enabled for a system running NTP in a network where there is a high security demand. This feature enhances the network security by means of client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.

## Configuration Prerequisites

The configuration of NTP authentication involves configuration tasks to be implemented on the client and on the server.

When configuring the NTP authentication feature, pay attention to the following principles:

- For all synchronization modes, when you enable the NTP authentication feature, you should configure an authentication key and specify it as a trusted key. Namely, the **ntp-service authentication enable** command must work together with the **ntp-service authentication-keyid** command and the **ntp-service reliable authentication-keyid** command. Otherwise, the NTP authentication function cannot be normally enabled.
- For the client/server mode or symmetric mode, you need to associate the specified authentication key on the client (symmetric-active peer if in the symmetric peer mode) with the corresponding NTP server (symmetric-passive peer if in the symmetric peer mode). Otherwise, the NTP authentication feature cannot be normally enabled.
- For the broadcast server mode or multicast server mode, you need to associate the specified authentication key on the broadcast server or multicast server with the corresponding NTP server. Otherwise, the NTP authentication feature cannot be normally enabled.
- For the client/server mode, if the NTP authentication feature has not been enabled for the client, the client can synchronize with the server regardless of whether the NTP authentication feature has been enabled for the server or not. If the NTP authentication is enabled on a client, the client can be synchronized only to a server that can provide a trusted authentication key.
- For all synchronization modes, the server side and the client side must be consistently configured.

## Configuration Procedure

### Configuring NTP authentication for a client

Follow these steps to configure NTP authentication for a client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable NTP authentication | **ntp-service authentication enable** | Required<br>Disabled by default |
| Configure an NTP authentication key | **ntp-service authentication-keyid** *keyid* **authentication-mode md5** *value* | Required<br>No NTP authentication key by default |
| Configure the key as a trusted key | **ntp-service reliable authentication-keyid** *keyid* | Required<br>No authentication key is configured to be trusted by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Associate the specified key with an NTP server | Client/server mode:<br>**ntp-service unicast-server** { *ip-address* \| *server-name* } **authentication-keyid** *keyid* | Required<br>You can associate a non-existing key with an NTP server. To enable NTP authentication, you must configure the key and specify it as a trusted key after associating the key with the NTP server. |
| | Symmetric peers mode:<br>**ntp-service unicast-peer** { *ip-address* \| *peer-name* } **authentication-keyid** *keyid* | |

**Note**

After you enable the NTP authentication feature for the client, make sure that you configure for the client an authentication key that is the same as on the server and specify that the authentication key is trusted; otherwise, the client cannot be synchronized to the server.

### Configuring NTP authentication for a server

Follow these steps to configure NTP authentication for a server:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable NTP authentication | **ntp-service authentication enable** | Required<br>Disabled by default |
| Configure an NTP authentication key | **ntp-service authentication-keyid** *keyid* **authentication-mode md5** *value* | Required<br>No NTP authentication key by default |
| Configure the key as a trusted key | **ntp-service reliable authentication-keyid** *keyid* | Required<br>No authentication key is configured to be trusted by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Associate the specified key with an NTP server | Broadcast server mode:<br>**ntp-service broadcast-server authentication-keyid** *keyid* | Required<br>You can associate a non-existing key with an NTP server. To enable NTP authentication, you must configure the key and specify it as a trusted key after associating the key with the NTP server. |
| | Multicast server mode:<br>**ntp-service multicast-server authentication-keyid** *keyid* | |

**Note**

The procedure of configuring NTP authentication on a server is the same as that on a client, and the same authentication key must be configured on both the server and client sides.

# Displaying and Maintaining NTP

| To do… | Use the command… | Remarks |
|---|---|---|
| View the information of NTP service status | **display ntp-service status** | Available in any view |
| View the information of NTP sessions | **display ntp-service sessions** [ **verbose** ] | Available in any view |
| View the brief information of the NTP servers from the local device back to the primary reference source | **display ntp-service trace** | Available in any view |

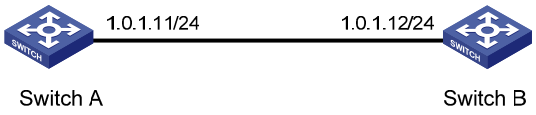
# NTP Configuration Examples

## Configuring NTP Client/Server Mode

### Network requirements

- The local clock of Switch A is to be used as a master clock, with the stratum level of 2.
- Switch B works in the client/server mode and Switch A is to be used as the NTP server of Switch B.

**Figure 1-7** Network diagram for NTP client/server mode configuration




### Configuration procedure

# View the NTP status of Switch B before clock synchronization.

```
<SwitchB> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
```

```
 Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

# Specify Switch A as the NTP server of Switch B so that Switch B is synchronized to Switch A.

```
<SwitchB> system-view
[SwitchB] ntp-service unicast-server 1.0.1.11
```

# View the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 1.05 ms
 Peer dispersion: 7.81 ms
 Reference time: 14:53:27.371 UTC Sep 19 2005 (C6D94F67.5EF9DB22)
```

As shown above, Switch B has been synchronized to Switch A, and the clock stratum level of Switch B is 3, while that of Switch A is 2.

# View the NTP session information of Switch B, which shows that an association has been set up between Switch B and Switch A.

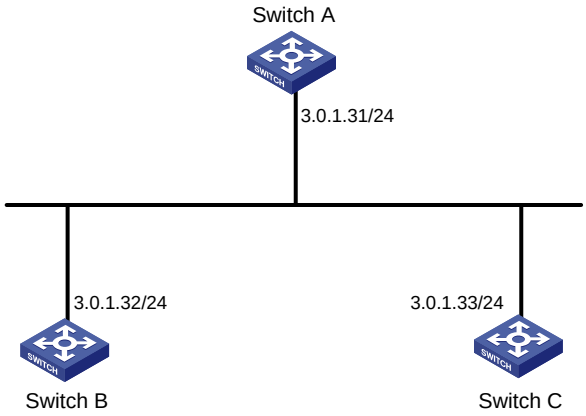
```
[SwitchB] display ntp-service sessions
      source      reference   stra  reach  poll  now  offset  delay  disper
**************************************************************************
[12345] 1.0.1.11  127.127.1.0    2    63    64    3    -75.5    31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

## Configuring the NTP Symmetric Mode

### Network requirements

- The local clock of Switch A is to be used as the master clock, with a stratum level of 2.
- Switch B works in the client mode and Switch A is to be used as the NTP server of Switch B.
- Switch C works in the symmetric-active mode and Switch B will act as peer of Switch C. Switch C is the symmetric-active peer while Switch B is the symmetric-passive peer.

**Figure 1-8** Network diagram for NTP symmetric peers mode configuration




## Configuration procedure

1) Configuration on Switch B:

# Specify Switch A as the NTP server of Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service unicast-server 3.0.1.31
```

2) Configuration on Switch C (after Switch B is synchronized to Switch A):

# Specify the local clock as the reference source, with the stratum level of 1.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 1
```

# Configure Switch B as a symmetric peer after local synchronization.

```
[SwitchC] ntp-service unicast-peer 3.0.1.32
```

In the step above, Switch B and Switch C are configured as symmetric peers, with Switch C in the symmetric-active mode and Switch B in the symmetric-passive mode. Because the stratus level of Switch C is 1 while that of Switch B is 3, Switch B is synchronized to Switch C.

# View the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.33
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: -21.1982 ms
 Root delay: 15.00 ms
 Root dispersion: 775.15 ms
 Peer dispersion: 34.29 ms
 Reference time: 15:22:47.083 UTC Sep 19 2005 (C6D95647.153F7CED)
```

As shown above, Switch B has been synchronized to Switch C, and the clock stratum level of Switch B is 2, while that of Switch C is 1.

# View the NTP session information of Switch B, which shows that an association has been set up between Switch B and Switch C.

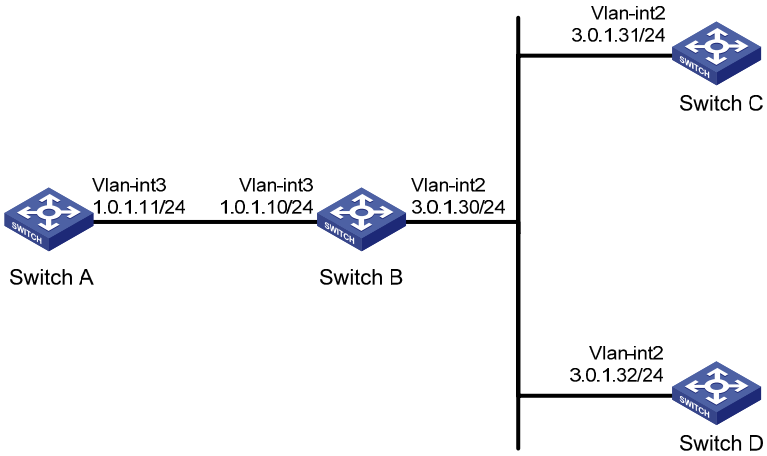
```
[SwitchB] display ntp-service sessions
       source     reference   stra  reach  poll  now   offset delay  disper
**************************************************************************
[245] 3.0.1.31  127.127.1.0    2    15    64   24   10535.0  19.6   14.5
[1234] 3.0.1.33   LOCL          1    14    64   27    -77.0   16.0   14.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  2
```

## Configuring NTP Broadcast Mode

### Network requirements

- The local clock of Switch C is to be used as the master clock, with a stratum level of 2.
- Switch C works in the broadcast server mode and sends out broadcast messages from VLAN-interface 2.
- Switch A and Switch D work in the broadcast client mode. Switch A listens to broadcast messages through its VLAN-interface 3 and Switch D from its VLAN-interface 2.

**Figure 1-9** Network diagram for NTP broadcast mode configuration




### Configuration procedure

1) Configuration on Switch C:

# Configure Switch C to work in the broadcast server mode and send broadcast messages through VLAN-interface 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```

2) Configuration on Switch D:

# Configure Switch D to work in the broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service broadcast-client
```

3) Configuration on Switch A:

# Configure Switch A to work in the broadcast client mode and receive broadcast messages on VLAN-interface 3.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service broadcast-client
```

Because Switch A and Switch C are on different subnets, Switch A cannot receive the broadcast messages from Switch C. Switch D gets synchronized upon receiving a broadcast message from Switch C.

# View the NTP status of Switch D after clock synchronization.

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

As shown above, Switch D has been synchronized to Switch C, and the clock stratum level of Switch D is 3, while that of Switch C is 2.

# View the NTP session information of Switch D, which shows that an association has been set up between Switch D and Switch C.

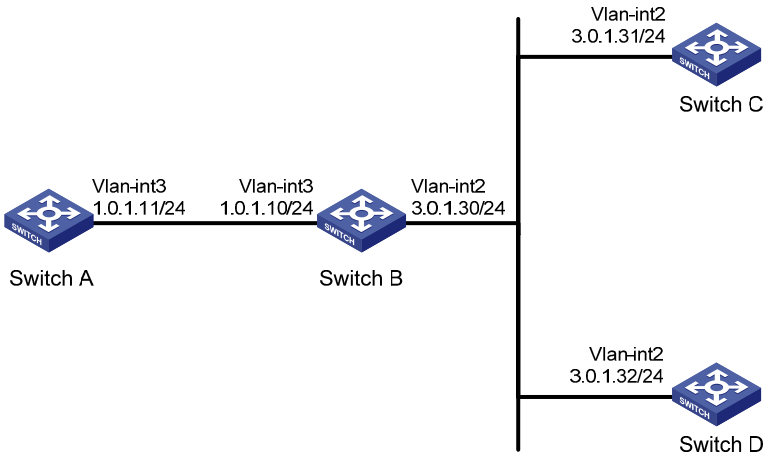
```
[SwitchD-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   2   254     64    62   -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

## Configuring NTP Multicast Mode

### Network requirements

- The local clock of Switch C is to be used as the master clock, with a stratum level of 2.
- Switch C works in the multicast server mode and sends out multicast messages from VLAN-interface 2.
- Switch A and Switch D work in the multicast client mode and receive multicast messages through VLAN-interface 3 and VLAN-interface 2 respectively.

**Figure 1-10** Network diagram for NTP multicast mode configuration




## Configuration procedure

1) Configuration on Switch C:

# Configure Switch C to work in the multicast server mode and send multicast messages through VLAN-interface 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

2) Configuration on Switch D:

# Configure Switch D to work in the multicast client mode and receive multicast messages on VLAN-interface 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

Because Switch D and Switch C are on the same subnet, Switch D can receive the multicast messages from Switch C without being enabled with the multicast functions and can be synchronized to Switch C.

# View the NTP status of Switch D after clock synchronization.

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

As shown above, Switch D has been synchronized to Switch C, and the clock stratum level of Switch D is 3, while that of Switch C is 2.

# View the NTP session information of Switch D, which shows that an association has been set up between Switch D and Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   2   254     64    62   -16.0    31.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

3) Configuration on Switch B:

Because Switch A and Switch C are on different subnets, you must enable the multicast functions on Switch B before Switch A can receive multicast messages from Switch C.

# Enable IP multicast routing and IGMP.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

4) Configuration on Switch A:

# Enable IP multicast routing and IGMP.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
```

# Configure Switch A to work in the multicast client mode and receive multicast messages on VLAN-interface 3.

```
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

# View the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 40.00 ms
 Root dispersion: 10.83 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:02:49.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

As shown above, Switch A has been synchronized to Switch C, and the clock stratum level of Switch A is 3, while that of Switch C is 2.

# View the NTP session information of Switch A, which shows that an association has been set up between Switch A and Switch C.

```
[SwitchA-Vlan-interface3] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0    2   255     64    26   -16.0    40.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

---

**Note**

Refer to *IGMP Configuration* in the *IP Multicast* volume for how to configure IGMP and PIM.

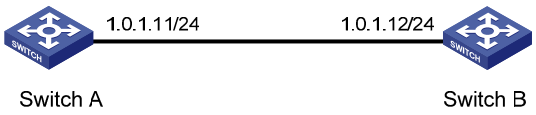
---

## Configuring NTP Client/Server Mode with Authentication

### Network requirements

- The local clock of Switch A is to be used as the master clock, with a stratum level of 2.
- Switch B works in the client mode and Switch A is to be used as the NTP server of Switch B, with Switch B as the client.
- NTP authentication is to be enabled on both Switch A and Switch B.

**Figure 1-11** Network diagram for configuration of NTP client/server mode with authentication




### Configuration procedure

Configuration on Switch B:

# Enable NTP authentication on Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service authentication enable
```

# Set an authentication key.

```
[SwitchB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

# Specify the key as a trusted key.

```
[SwitchB] ntp-service reliable authentication-keyid 42
```

# Specify Switch A as the NTP server.

```
[SwitchB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Before Switch B can synchronize its clock to that of Switch A, you need to enable NTP authentication for Switch A.

Perform the following configuration on Switch A:

# Enable NTP authentication.

```
[SwitchA] ntp-service authentication enable
```

# Set an authentication key.

```
[SwitchA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

# Specify the key as a trusted key.

```
[SwitchA] ntp-service reliable authentication-keyid 42
```

# View the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 1.05 ms
 Peer dispersion: 7.81 ms
 Reference time: 14:53:27.371 UTC Sep 19 2005 (C6D94F67.5EF9DB22)
```

As shown above, Switch B has been synchronized to Switch A, and the clock stratum level of Switch B is 3, while that of Switch A is 2.

# View the NTP session information of Switch B, which shows that an association has been set up Switch B and Switch A.

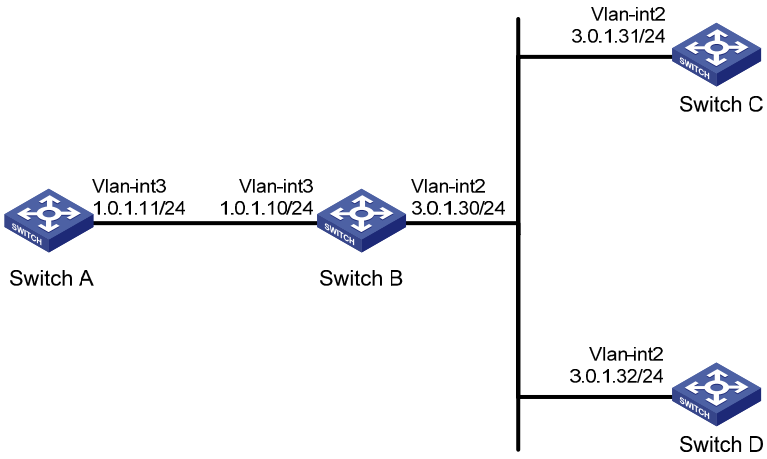
```
[SwitchB] display ntp-service sessions
      source      reference   stra  reach  poll  now  offset  delay  disper
**************************************************************************
[12345] 1.0.1.11  127.127.1.0    2    63    64    3    -75.5    31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

## Configuring NTP Broadcast Mode with Authentication

### Network requirements

- The local clock of Switch C is to be used as the master clock, with a stratum level of 3.
- Switch C works in the broadcast server mode and sends out broadcast messages from VLAN-interface 2.
- Switch D works in the broadcast client mode and receives broadcast messages through VLAN-interface 2.
- NTP authentication is enabled on both Switch C and Switch D.

**Figure 1-12** Network diagram for configuration of NTP broadcast mode with authentication




## Configuration procedure

1) Configuration on Switch C:

# Configure NTP authentication.

```
<SwitchC> system-view
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 123456
[SwitchC] ntp-service reliable authentication-keyid 88
```

# Specify Switch C as an NTP broadcast server, and specify an authentication key.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

2) Configuration on Switch D:

# Configure NTP authentication.

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 88 authentication-mode md5 123456
[SwitchD] ntp-service reliable authentication-keyid 88
```

# Configure Switch D to work in the NTP broadcast client mode.

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service broadcast-client
```

Now, Switch D can receive broadcast messages through VLAN-interface 2, and Switch C can send broadcast messages through VLAN-interface 2. Upon receiving a broadcast message from Switch C, Switch D synchronizes its clock to that of Switch C.

# View the NTP status of Switch D after clock synchronization.

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
```

```
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

As shown above, Switch D has been synchronized to Switch C, and the clock stratum level of Switch D is 4, while that of Switch C is 3.

# View the NTP session information of Switch D, which shows that an association has been set up between Switch D and Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   3   254     64    62   -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

# Table of Contents

# 1 Hotfix Configuration

When configuring hotfix, go to these sections for information you are interested in:



## Hotfix Overview

Hotfix is a fast and cost-effective method to repair software defects of a switch. Compared with another method, software version upgrade, hotfix can upgrade the software without interrupting the running services of the switch, that is, it can repair the software defects of the current version without rebooting the switch.

### Basic Concepts in Hotfix

#### Patch and patch file

A patch, also called patch unit, is a package to fix software defects. Generally, patches are released as patch files. A patch file may contain one or more patches for different defects. After loaded from the Flash to the memory patch area, each patch is assigned a unique number, which starts from 1, for identification, management and operation. For example, if a patch file has three patch units, they will be numbered as 1, 2, and 3 respectively.

#### Incremental patch

Patches in a patch file are all incremental patches. An incremental patch means that the patch is dependent on the previous patch units. For example, if a patch file has three patch units, patch 3 can be running only after patch 1 and 2 take effect. You cannot run patch 3 separately.

#### Common patch and temporary patch

Patches fall into two types, common patches and temporary patches.

- Common patches are those formally released through the version release flow.
- Temporary patches are those not formally released through the version release flow, but temporarily provided to solve the emergent problems.

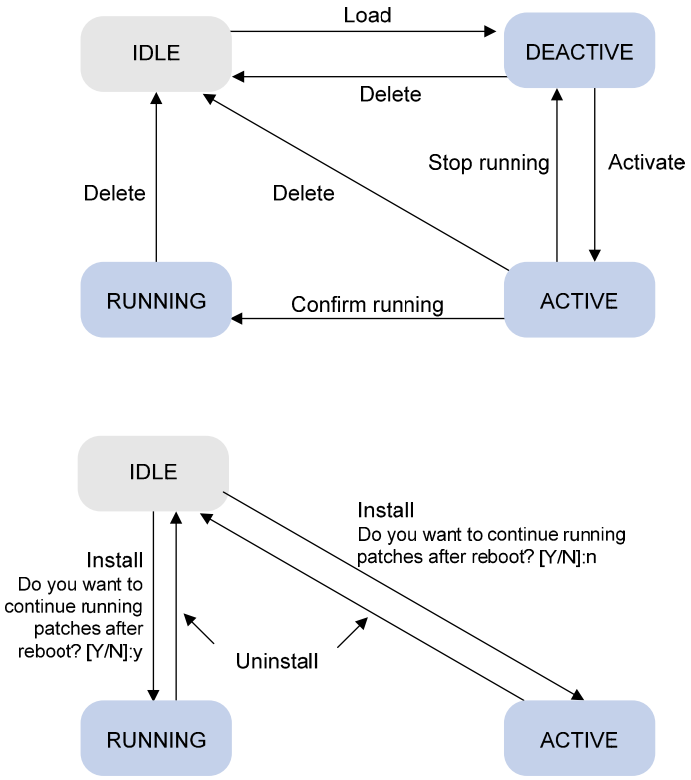
The common patches always include the functions of the previous temporary patches, so as to replace them. The patch type affects the patch loading process only: the system will delete all the temporary patches before it loads the common patch.

### Patch Status

Each patch has its status, which can be switched by command lines. The relationship between patch state changes and command actions is shown in Figure 1-1. The patch can be in the state of IDLE, DEACTIVE, ACTIVE, and RUNNING. Load, run temporarily, confirm running, stop running, delete,

install, and uninstall represent operations, corresponding to commands of **patch load**, **patch active**, **patch run**, **patch deactive**, **patch delete**, **patch install**, and **undo patch install**. For example, if you execute the **patch active** command for the patches in the DEACTIVE state, the patches turn to the ACTIVE state.

**Figure 1-1** Relationship between patch state changes and command actions




**Note**

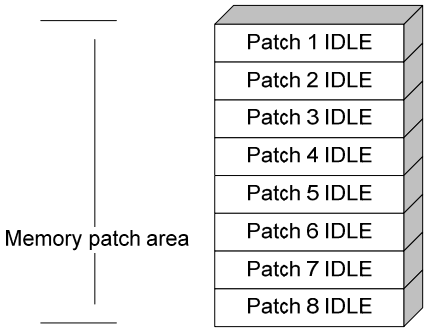
Information about patch states is saved in file **patchstate** on the flash. It is recommended not to operate this file.

### IDLE state

Patches in the IDLE state are not loaded. You cannot install or run the patches, as shown in Figure 1-2 (suppose the memory patch area can load up to eight patches).

The patches that are in the IDLE state will be still in the IDLE state after system reboot.

**Figure 1-2** Patches are not loaded to the memory patch area




**Note**

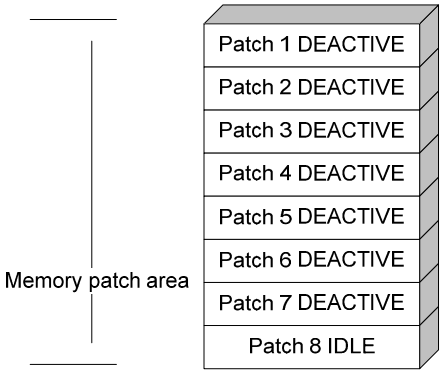
Currently, the system patch area supports up to 200 patches.

## DEACTIVE state

Patches in the DEACTIVE state have been loaded to the memory patch area but have not run in the system yet. Suppose that there are seven patches in the patch file to be loaded. After the seven patches successfully pass the version check and CRC check, they will be loaded to the memory patch area and are in the DEACTIVE state. At this time, the patch states in the system are as shown in Figure 1-3.

The patches that are in the DEACTIVE state will be still in the DEACTIVE state after system reboot.

**Figure 1-3** A patch file is loaded to the memory patch area

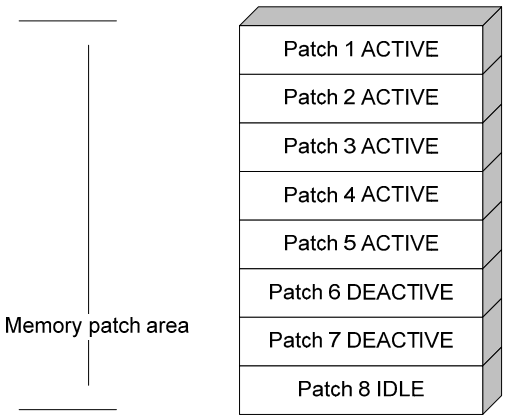



## ACTIVE state

Patches in the ACTIVE state are those that have run temporarily in the system and will become DEACTIVE after system reboot. For the seven patches in Figure 1-3, if you activate the first five patches, the state of them will change from DEACTIVE to ACTIVE. At this time, the patch states in the system are as shown in Figure 1-4.

The patches that are in the ACTIVE state will be in the DEACTIVE state after system reboot.

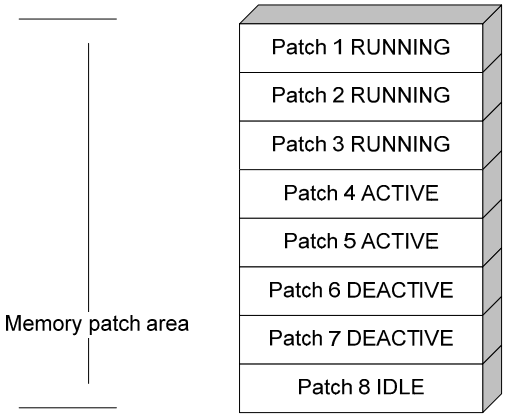
**Figure 1-4** Patches are activated




### RUNNING state

After you confirm the running of the ACTIVE patches, the state of the patches will become RUNNING and will be in the RUNNING state after system reboot. For the five patches in Figure 1-4, if you confirm the running the first three patches, their states will change from ACTIVE to RUNNING. At this time, the patch states of the system are as shown in Figure 1-5.

**Figure 1-5** Patches are running




The patches that are in the RUNNING state will be still in the RUNNING state after system reboot.

## Hotfix Configuration Task List

| Task | | Remarks |
|---|---|---|
| Install patches | One-Step Patch Installation | Use either approach.<br>The step-by-step patch installation allows you to control the patch status. |
| | Step-by-Step Patch Installation | |
| Uninstall patches | One-Step Patch Uninstallation | Use either approach.<br>The step-by-step patch uninstallation allows you to control the patch status. |
| | Step-by-Step Patch Uninstallation | |

## Configuration Prerequisites

Patches are released per device model. Before patching the system, you need to save the appropriate patch files to the flash of the switch using FTP or TFTP. When saving the patch files, note that:

- The patch files match the switch model and software version. If they are not matched, the hotfixing operation will fail.
- Name the patch file properly. Otherwise, the system cannot locate the patch file and the hotfixing operation will fail. The name is in the format of "patch_*PATCH-FLAG suffix*.bin". The first three characters of the version item (using the **display patch information** command) represent the PATCH-FLAG suffix. The system searches the root directory of the Flash for patch files based on the PATCH-FLAG. If there is a match, the system loads patches to or install them on the memory patch area.

Table 1-1 describes the default patch name for each board type.

**Table 1-1** Patch names for divice

| Product | Board type | PATCH-FLAG | Default patch name |
|---|---|---|---|
| 4500G | — | PATCH-XXX | patch_xxx.bin |

## One-Step Patch Installation

You can use the **patch install** command to install patches in one step. After you execute the command, the system displays the message "Do you want to continue running patches after reboot? [Y/N]:".

- Entering **y** or **Y**: All the specified patches are installed, and turn to the RUNNING state from IDLE. This equals execution of the commands **patch location**, **patch load**, **patch active**, and **patch run**. The patches remain RUNNING after system reboot.
- Entering **n** or **N**: All the specified patches are installed and turn to the ACTIVE state from IDLE. This equals execution of the commands **patch location**, **patch load** and **patch active**. The patches turn to the DEACTIVE state after system reboot.

Follow these steps to install the patches in one step:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Install the patches in one step | **patch install** *patch-location* | Required |

**Note**

- The patch matches the switch type and software version.
- The **patch install** command changes the patch file location specified with the **patch location** command to the directory specified by the *patch-location* argument of the **patch install** command.

# Step-by-Step Patch Installation

## Step-by-Step Patch Installation Task List

| Task | Remarks |
|---|---|
| Configuring the Patch File Location | Optional |
| Loading a Patch File | Required |
| Activating Patches | Required |
| Confirming Running Patches | Optional |

## Configuring the Patch File Location

Follow these steps to configure the patch file location:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the patch file location | **patch location** *patch-location* | Optional<br>**flash:** by default |

**Note**

The **patch install** command changes patch file location specified with the **patch location** command to the directory specified by the *patch-location* argument of the **patch install** command. For example, if you execute the **patch location** *xxx* command and then the **patch install** *yyy* command, the patch file location automatically changes from xxx to yyy.

## Loading a Patch File

Loading the right patch files is the basis of other hotfixing operations. The system loads a patch file from the flash by default.

**Caution**

Set the file transfer mode to binary mode before using FTP or TFTP to upload/download patch files to/from the flash of the switch. Otherwise, patch file cannot be parsed properly.

Follow the steps below to load a patch file:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Load the patch file from the flash to the memory patch area | **patch load** | Required |

### Activating Patches

After you activate a patch, the patch will take effect and is in the test-run stage. After the switch is reset or rebooted, the patch becomes invalid.

If you find that an ACTIVE patch is of some problem, you can reboot the switch to deactivate the patch, so as to avoid a series of running faults resulting from patch error.

Follow the steps below to activate patches:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Activate the specified patches | **patch active** *patch-number* | Required |

### Confirming Running Patches

After you confirm the running of a patch, the patch state becomes RUNNING, and the patch is in the normal running stage. After the switch is reset or rebooted, the patch is still valid.

Follow the steps below to confirm the running of the patches:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Confirm the running of the specified patches | **patch run** *patch-number* | Required |

**Note**

This operation is applicable to patches in the ACTIVE state only.

## One-Step Patch Uninstallation

- On a centralized device

You can use the **undo patch install** command to uninstall all patches. The patches then turn to the IDLE state. This equals execution of the commands **patch deactive** and **patch delete**.

- On a distributed device

You can use the **undo patch install** command to uninstall all patches from all the boards and OAM CPU. The patches then turn to the IDLE state. This equals the execution of the commands **patch deactive** and **patch delete** on each board and OAM CPU.

- On a centralized stacking device

You can use the **undo patch install** command to uninstall patches from all the member devices. The patches then turn to the IDLE state. This equals the execution of the commands **patch deactive** and **patch delete** on each member device.

Follow these steps to uninstall the patches in one step:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Uninstall the patches | **undo patch install** | Required |

# Step-by-Step Patch Uninstallation

## Step-by-Step Patch Uninstallation Task List

| Task | Remarks |
|---|---|
| Stop Running Patches | Required |
| Deleting Patches | Required |

## Stop Running Patches

After you stop running a patch, the patch state becomes DEACTIVE, and the system runs in the way before it is installed with the patch.

Follow the steps below to stop running patches:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Stop running the specified patches | **patch deactive** *patch-number* | Required |

## Deleting Patches

Deleting patches only removes the patches from the memory patch area, and does not delete them from the storage medium. The patches turn to IDLE state after this operation. After a patch is deleted, the system runs in the way before it is installed with the patch.

Follow the steps below to delete patches:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Delete the specified patches from the memory patch area | **patch delete** *patch-number* | Required |

# Displaying and Maintaining Hotfix

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the patch information | **display patch information** | Available in any view |

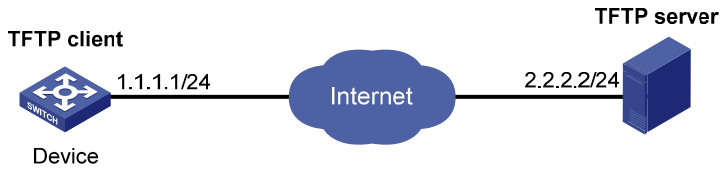
# Hotfix Configuration Examples

## Hotfix Configuration Example

### Network requirements

- The software running on Device is of some problem, and thus hotfixing is needed.
- The patch file **patch_xxx.bin** is saved on the TFTP server.
- The IP address of Device is 1.1.1.1/24, and IP address of TFTP Server is 2.2.2.2/24. An available route exists between Device and TFTP server.

**Figure 1-6** Network diagram of hotfix configuration




### Configuration procedure

1) Configure TFTP Server. Note that the configuration varies depending on server type and the configuration procedure is omitted.
- Enable the TFTP server function.
- Save the patch file **patch_xxx.bin** to the directory of the TFTP server.

2) Configure Device

---

**Caution**

Make sure the free flash space of the switch is big enough to store the patch file.

---

# Before upgrading the software, use the **save** command to save the current system configuration. The configuration procedure is omitted.

# Load the patch file **patch_xxx.bin** from the TFTP server to the root directory of the Flash.

```
<Device> tftp 2.2.2.2 get patch_xxx.bin
```

# Install the patch.

```
<Device> system-view
[Device] patch install flash:
Patches will be installed. Continue? [Y/N]:y
Do you want to continue running patches after reboot? [Y/N]:y
```

```
Installing patches........
Installation completed, and patches will continue to run after reboot.
```

# Table of Contents

# 1 Cluster Management Configuration

When configuring cluster management, go to these sections for information you are interested in:



## Cluster Management Overview

### Cluster Management Definition

A cluster is a group of network devices. Cluster management is to implement management of large numbers of distributed network devices. Cluster management offers the following advantages:

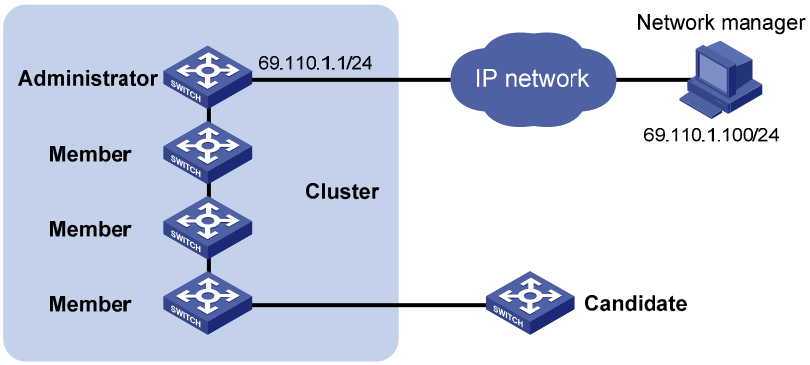
- Saving public IP address resource
- Simplifying configuration and management tasks. By configuring a public IP address on one device, you can configure and manage a group of devices without the trouble of logging in to each device separately.
- Providing topology discovery and display function, which is useful for network monitoring and debugging
- Allowing simultaneous software upgrading and parameter configuration on multiple devices, free of topology and distance limitations

### Roles in a Cluster

The devices in a cluster play different roles according to their different functions and status. You can specify the following three roles for the devices:

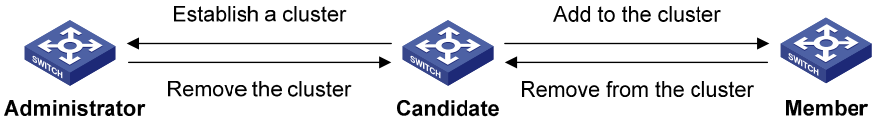
- Management device (Administrator): The device providing management interfaces for all devices in a cluster and the only device configured with a public IP address. You can specify one and only one management device for a cluster. Any configuration, management, and monitoring of the other devices in a cluster can only be implemented through the management device. When a device is specified as the management device, it collects related information to discover and define candidate devices.
- Member device (Member): A device managed by the management device in a cluster.
- Candidate device (Candidate): A device that does not belong to any cluster but can be added to a cluster. Different from a member device, its topology information has been collected by the management device but it has not been added to the cluster.

**Figure 1-1** Network diagram for a cluster




As shown in Figure 1-1, the device configured with a public IP address and performs the management function is the management device, the other managed devices are member devices, and the device that does not belong to any cluster but can be added to a cluster is a candidate device. The management device and the member devices form the cluster.

**Figure 1-2** Role change in a cluster




As shown in Figure 1-2, a device in a cluster changes its role according to the following rules:

- A candidate device becomes a management device when you create a cluster on it. A management device becomes a candidate device only after the cluster is removed.
- A candidate device becomes a member device after being added to a cluster. A member device becomes a candidate device after it is removed from the cluster.

## How a Cluster Works

Cluster management is implemented through HW Group Management Protocol version 2 (HGMPv2), which consists of the following three protocols:

- Neighbor Discovery Protocol (NDP)
- Neighbor Topology Discovery Protocol (NTDP)
- Cluster

A cluster configures and manages the devices in it through the above three protocols. Cluster management involves topology information collection and the establishment and maintenance of a cluster. Topology information collection and cluster maintenance are independent from each other, with the former starting before the cluster is created:

- All devices use NDP to collect the information of the directly connected neighbors, including their software version, host name, MAC address and port number.
- The management device uses NTDP to collect the information of the devices within user-specified hops and the topology information of all devices and specify the candidate devices of the cluster.
- The management device adds or deletes a member device and modifies cluster management configuration according to the candidate device information collected through NTDP.

## Introduction to NDP

NDP is used to discover the information about directly connected neighbors, including the device name, software version, and connecting port of the adjacent devices. NDP works in the following ways:

- A device running NDP periodically sends NDP packets to its neighbors. An NDP packet carries NDP information (including the device name, software version, and connecting port, etc.) and the holdtime, which indicates how long the receiving devices will keep the NDP information. At the same time, the device also receives (but does not forward) the NDP packets from its neighbors.
- A device running NDP stores and maintains an NDP table. The device creates an entry in the NDP table for each neighbor. If a new neighbor is found, meaning the device receives an NDP packet sent by the neighbor for the first time, the device adds an entry in the NDP table. If the NDP information carried in the NDP packet is different from the stored information, the corresponding entry and holdtime in the NDP table are updated; otherwise, only the holdtime of the entry is updated. If no NDP information from the neighbor is received when the holdtime times out, the corresponding entry is removed from the NDP table.

NDP runs on the data link layer, and therefore supports different network layer protocols.

## Introduction to NTDP

NTDP provides information required for cluster management; it collects topology information about the devices within the specified hop count. Based on the neighbor information stored in the neighbor table maintained by NDP, NTDP on the management device advertises NTDP topology collection requests to collect the NDP information of all the devices in a specific network range as well as the connection information of all its neighbors. The information collected will be used by the management device or the network management software to implement required functions.

When a member device detects a change on its neighbors through its NDP table, it informs the management device through handshake packets. Then the management device triggers its NTDP to collect specific topology information, so that its NTDP can discover topology changes timely.

The management device collects topology information periodically. You can also administratively launch a topology information collection. The process of topology information collection is as follows:

- The management device periodically sends NTDP topology collection request from the NTDP-enabled ports.
- Upon receiving the request, the device sends NTDP topology collection response to the management device, copies this response packet on the NTDP-enabled port and sends it to the adjacent device. Topology collection response includes the basic information of the NDP-enabled device and NDP information of all adjacent devices.
- The adjacent device performs the same operation until the NTDP topology collection request is sent to all the devices within specified hops.

When the NTDP topology collection request is advertised in the network, large numbers of network devices receive the NTDP topology collection request and send NTDP topology collection response at the same time, which may cause congestion and the management device busyness. To avoid such case, the following methods can be used to control the speed of the NTDP topology collection request advertisement:

- Upon receiving an NTDP topology collection request, each device does not forward it, instead, it waits for a period of time and then forwards the NTDP topology collection request on the first NTDP-enabled port.
- On the same device, except the first port, each NTDP-enabled port waits for a period of time and

then forwards the NTDP topology collection request after its prior port forwards the NTDP topology collection request.

### Cluster management maintenance

1) Adding a candidate device to a cluster

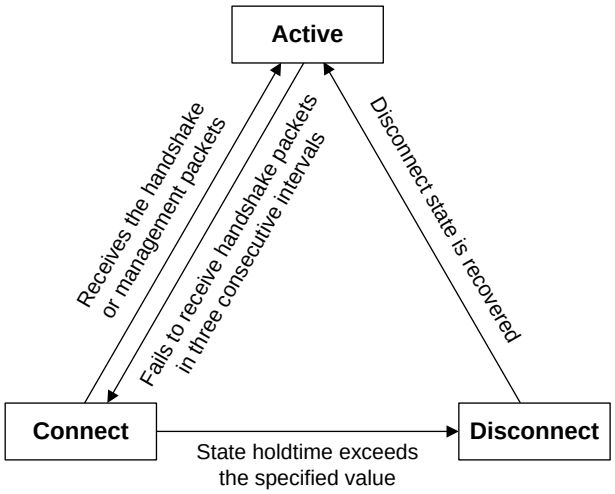
You should specify the management device before creating a cluster. The management device discovers and defines a candidate device through NDP and NTDP protocols. The candidate device can be automatically or manually added to the cluster.

After the candidate device is added to the cluster, it can obtain the member number assigned by the management device and the private IP address used for cluster management.

2) Communication within a cluster

In a cluster the management device communicates with its member devices by sending handshake packets to maintain connection between them. The management/member device state change is shown in Figure 1-3.

**Figure 1-3** Management/member device state change




- After a cluster is created, a candidate device is added to the cluster and becomes a member device, the management device saves the state information of its member device and identifies it as Active. And the member device also saves its state information and identifies itself as Active.
- After a cluster is created, its management device and member devices begin to send handshake packets. Upon receiving the handshake packets from the other side, the management device or a member device simply remains its state as Active, without sending a response.
- If the management device does not receive the handshake packets from a member device in an interval three times of the interval to send handshake packets, it changes the status of the member device from Active to Connect. Likewise, if a member device fails to receive the handshake packets from the management device in an interval three times of the interval to send handshake packets, the status of itself will also be changed from Active to Connect.
- If this management device, in information holdtime, receives the handshake or management packets from its member device which is in Connect state, it changes the state of its member device to Active; otherwise, it changes the state of its member device to Disconnect, in which case the management device considers its member device disconnected. If this member device, which is in Connect state, receives handshake or management packets from the management device in information holdtime, it changes its state to Active; otherwise, it changes its state to Disconnect.
- If the communication between the management device and a member device is recovered, the

member device which is in Disconnect state will be added to the cluster. After that, the state of the member device locally and on the management device will be changed to Active.

Besides, a member device informs the management device using handshake packets when there is a neighbor topology change.

### Management VLAN

The management VLAN is a VLAN used for communication in a cluster; it limits the cluster management range. Through configuration of the management VLAN, the following functions can be implemented:

- Management packets (including NDP, NTDP and handshake packets) are restricted within the management VLAN, therefore isolated from other packets, which enhances security.
- The management device and the member devices communicate with each other through the management VLAN.

For a cluster to work normally, you must set the packets from the management VLAN to pass the ports connecting the management device and the member/candidate devices (including the cascade ports). Therefore:

- If the packets from the management VLAN cannot pass a port, the device connected with the port cannot be added to the cluster. Therefore, if the ports (including the cascade ports) connecting the management device and the member/candidate devices prohibit the packets from the management VLAN, you can set the packets from the management VLAN to pass the ports on candidate devices with the management VLAN auto-negotiation function.
- Only when the default VLAN ID of the cascade ports and the ports connecting the management device and the member/candidate devices is that of the management VLAN can you set the packets without tags from the management VLAN to pass the ports; otherwise, only the packets with tags from the management VLAN can pass the ports.

---

**Note**

- If a candidate device is connected to a management device through another candidate device, the ports between the two candidate devices are cascade ports.
- For information about VLAN, refer to *VLAN Configuration* in the *Access Volume*.

---

## Cluster Configuration Task List

Before configuring a cluster, you need to determine the roles and functions the devices play. You also need to configure the related functions, preparing for the communication between devices within the cluster.

Complete these tasks to configure a cluster:

| Task | | Remarks |
|---|---|---|
| Configuring the Management Device | Enabling NDP Globally and for Specific Ports | Optional |
| | Configuring NDP Parameters | Optional |
| | Enabling NTDP Globally and for Specific Ports | Optional |
| | Configuring NTDP Parameters | Optional |
| | Manually Collecting Topology Information | Optional |
| | Enabling the Cluster Function | Optional |
| | Establishing a Cluster | Required |
| | Enabling Management VLAN Auto-negotiation | Required |
| | Configuring Communication Between the Management Device and the Member Devices Within a Cluster | Optional |
| | Configuring Cluster Management Protocol Packets | Optional |
| | Cluster Member Management | Optional |
| Configuring the Member Devices | Enabling NDP | Optional |
| | Enabling NTDP | Optional |
| | Manually Collecting Topology Information | Optional |
| | Enabling the Cluster Function | Optional |
| | Deleting a Member Device from a Cluster | Optional |
| Configuring Access Between the Management Device and Its Member Devices | | Optional |
| Adding a Candidate Device to a Cluster | | Optional |
| Configuring Advanced Cluster Functions | Configuring Topology Management | Optional |
| | Configuring Interaction for a Cluster | Optional |
| | SNMP Configuration Synchronization Function | Optional |
| | Configuring Web User Accounts in Batches | Optional |

**Caution**

- Disabling the NDP and NTDP functions on the management device and member devices after a cluster is created will not cause the cluster to be dismissed, but will influence the normal operation of the cluster.
- When both the cluster function and the 802.1X function (or the MAC address authentication) are enabled on devices, you need to enable HABP on the devices. Otherwise, the management device of the cluster cannot manage the devices connected with it. For description of HABP, refer to *HABP Configuration* in the *Security Volume*.
- If the routing table of the management device is full when a cluster is established, that is, entries with the destination address as a candidate device cannot be added to the routing table, all candidate devices will be added to and removed from the cluster repeatedly.
- If the routing table of a candidate device is full when the candidate device is added to a cluster, that is, the entry with the destination address as the management device cannot be added to the routing table, the candidate device will be added to and removed from the cluster repeatedly.

# Configuring the Management Device

## Enabling NDP Globally and for Specific Ports

For NDP to work normally, you must enable NTDP both globally and on specific ports.

Follow these steps to enable NDP globally and for specific ports:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enable NDP globally | | **ndp enable** | Optional<br>Enabled by default. |
| Enable the NDP feature for the port(s) | In system view | **ndp enable interface***interface-list* | Use either command<br>By default, NDP is enabled globally and also on all ports. |
| | In Ethernet port view or Layer 2 aggregate interface view | **interface** *interface-type interface-number* | |
| | | **ndp enable** | |

**Note**

You are recommended to disable NDP on the port which connects with the devices that do not need to join the cluster, preventing the management device from adding the device which needs not to join the cluster and collecting the topology information of this device.

## Configuring NDP Parameters

A port enabled with NDP periodically sends NDP packets to its neighbors. If no NDP information from the neighbor is received when the holdtime times out, the corresponding entry is removed from the NDP table.

Follow these steps to configure NDP parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the interval for sending NDP packets | **ndp timer hello** *hello-time* | Optional<br>60 seconds by default. |
| Configure the period for the receiving device to keep the NDP packets | **ndp timer aging** *aging-time* | Optional<br>180 seconds by default. |

**Caution**

The time for the receiving device to hold NDP packets cannot be shorter than the interval for sending NDP packets; otherwise, the NDP table may become instable.

## Enabling NTDP Globally and for Specific Ports

For NTDP to work normally, you must enable NTDP both globally and on specific ports.

Follow these steps to enable NTDP globally and for specific ports:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable NTDP globally | **ntdp enable** | Optional<br>Enabled by default |
| Enable NTDP for the port | **interface** *interface-type interface-number* | Optional<br>NTDP is enabled on all ports by default. |
| | **ntdp enable** | |

**Note**

You are recommended to disable NTDP on the port which connects with the devices that do not need to join the cluster, preventing the management device from adding the device which needs not to join the cluster and collecting the topology information of this device.

## Configuring NTDP Parameters

By configuring the maximum hops for collecting topology information, you can get topology information

of the devices in a specified range, thus avoiding unlimited topology collection.

After the interval for collecting topology information is configured, the device collects the topology information at this interval.

To avoid network congestion caused by large amounts of topology responses received in short periods:

- Upon receiving an NTDP topology collection request, a device does not forward it, instead, it waits for a period of time and then forwards the NTDP topology collection request on its first NTDP-enabled port.
- On the same device, except the first port, each NTDP-enabled port waits for a period of time and then forwards the NTDP topology collection request after the previous port forwards the NTDP topology collection request.

Follow these steps to configure NTDP parameters:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the maximum hops for topology collection | **ntdp hop** *hop-value* | Optional<br>3 by default. |
| Configure the interval to collect topology information | **ntdp timer** *interval-time* | Optional<br>1 minute by default. |
| Configure the delay to forward topology-collection request packets on the first port | **ntdp timer hop-delay** *time* | Optional<br>200 ms by default. |
| Configure the port delay to forward topology collection request on other ports | **ntdp timer port-delay** *time* | Optional<br>20 ms by default. |

**Note**

The two delay values should be configured on the topology collecting device. A topology collection request sent by the topology collecting device carries the two delay values, and a device that receives the request forwards the request according to the delays.

## Manually Collecting Topology Information

The management device collects topology information periodically after a cluster is created. In addition, you can configure to manually initiate topology information collection, thus managing and monitoring the device on real time, regardless of whether a cluster is created.

Follow these steps to configure to manually collect topology information:

| To do… | Use the command… | Remarks |
|---|---|---|
| Manually collect topology information | **ntdp explore** | Required |

## Enabling the Cluster Function

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the cluster function globally | **cluster enable** | Optional<br>Enabled by default. |

## Establishing a Cluster

Before establishing a cluster, you need to specify the management VLAN, and you cannot modify the management VLAN after a device is added to the cluster.

In addition, you need to configure a private IP address pool for the devices to be added to the cluster on the device to be configured as the management device before establishing a cluster. Meanwhile, the IP addresses of the VLAN interfaces of the management device and member devices cannot be in the same network segment as that of the cluster address pool; otherwise, the cluster cannot work normally. When a candidate device is added to a cluster, the management device assigns it a private IP address for it to communicate with other devices in the cluster.

You can establish a cluster in two ways: manually and automatically. With the latter, you can establish a cluster according to the prompt information. The system:

1) Prompts you to enter a name for the cluster you want to establish;
2) Lists all the candidate devices within your predefined hop count;
3) Starts to automatically add them to the cluster.

You can press **Ctrl+C** anytime during the adding process to exit the cluster auto-establishment process. However, this will only stop adding new devices into the cluster, and devices already added into the cluster are not removed.

Follow these steps to manually establish a cluster:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Specify the management VLAN | | **management-vlan** *vlan-id* | Optional<br>By default, VLAN 1 is the management VLAN. |
| Enter cluster view | | **cluster** | — |
| Configure the private IP address range for member devices | | **ip-pool** *administrator-ip-address* { *mask* \| *mask-length* } | Required<br>Not configured by default. |
| Establish a cluster | Manually establish a cluster | **build** *name* | Required<br>Use either approach<br>By default, the device is not the management device. |
| | Automatically establish a cluster | **auto-build** [ **recover** ] | |

## Enabling Management VLAN Auto-negotiation

The management VLAN limits the cluster management range. If the device discovered by the management device does not belong to the management VLAN, meaning the cascade ports and the ports connecting with the management device do not allow the packets from the management VLAN to pass, and the new device cannot be added to the cluster. Through the configuration of the management VLAN auto-negotiation function, the cascade ports and the ports directly connected to the management device can be automatically added to the management VLAN.

Follow these steps to configure management VLAN auto-negotiation:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Enable management VLAN auto-negotiation | **management-vlan synchronization enable** | Required<br>Disabled by default. |

## Configuring Communication Between the Management Device and the Member Devices Within a Cluster

In a cluster, the management device and member devices communicate by sending handshake packets to maintain connection between them. You can configure interval of sending handshake packets and the holdtime of a device on the management device. This configuration applies to all member devices within the cluster. For a member device in Connect state:

- If the management device does not receive handshake packets from a member device within the holdtime, it changes the state of the member device to Disconnect. When the communication is recovered, the member device needs to be re-added to the cluster (this process is automatically performed).
- If the management device receives handshake packets from the member device within the holdtime, the state of the member device remains Active.

Follow these steps to configure communication between the management device and the member devices within a cluster:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure the interval to send handshake packets | **timer** *interval-time* | Optional<br>10 seconds by default |
| Configure the holdtime of a device | **holdtime** *seconds* | Optional<br>60 seconds by default |

## Configuring Cluster Management Protocol Packets

By default, the destination MAC address of cluster management protocol packets (including NDP, NTDP and HABP packets) is a multicast MAC address 0180-C200-000A, which IEEE reserved for later use. Since some devices cannot forward the multicast packets with the destination MAC address of

0180-C200-000A, cluster management packets cannot traverse these devices. For a cluster to work normally in this case, you can modify the destination MAC address of a cluster management protocol packet without changing the current networking.

The management device periodically sends MAC address negotiation broadcast packets to advertise the destination MAC address of the cluster management protocol packets.

Follow these steps to configure the destination MAC address of the cluster management protocol packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure the destination MAC address for cluster management protocol packets | **cluster-mac** *mac-address* | Required<br>The destination MAC address is 0180-C200-000A by default. |
| Configure the interval to send MAC address negotiation broadcast packets | **cluster-mac syn-interval** *interval-time* | Optional<br>One minute by default. |

**Caution**

When you configure the destination MAC address for cluster management protocol packets:

- If the interval for sending MAC address negotiation broadcast packets is 0, the system automatically sets it to 1 minute.
- If the interval for sending MAC address negotiation broadcast packets is not 0, the interval remains unchanged.

## Cluster Member Management

You can manually add a candidate device to a cluster, or remove a member device from a cluster.

If a member device needs to be rebooted for software upgrade or configuration update, you can remotely reboot it through the management device.

### Adding a member device

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Add a candidate device to the cluster | **add-member** [ *member-number* ] **mac-address** *mac-address* [ **password** *password* ] | Required |

### Removing a member device

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Remove a member device from the cluster | **delete-member** *member-number* [ **to-black-list** ] | Required |

### Rebooting a member device

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Reboot a specified member device | **reboot member** { *member-number* \| **mac-address** *mac-address* } [ **eraseflash** ] | Required |

# Configuring the Member Devices

## Enabling NDP

Refer to Enabling NDP Globally and for Specific Ports.

## Enabling NTDP

Refer to Enabling NTDP Globally and for Specific Ports.

## Manually Collecting Topology Information

Refer to Manually Collecting Topology Information.

## Enabling the Cluster Function

Refer to Enabling the Cluster Function.

## Deleting a Member Device from a Cluster

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Delete a member device from the cluster | **undo administrator-address** | Required |

# Configuring Access Between the Management Device and Its Member Devices

After having successfully configured NDP, NTDP and cluster, you can configure, manage and monitor

the member devices through the management device. You can manage member devices in a cluster through switching from the operation interface of the management device to that of a member device or configure the management device by switching from the operation interface of a member device to that of the management device.

Follow these steps to configure access between member devices of a cluster:

| To do… | Use the command… | Remarks |
|---|---|---|
| Switch from the operation interface of the management device to that of a member device | **cluster switch-to** { *member-number* \| **mac-address** *mac-address* \| **sysname** *member-sysname* } | Required |
| Switch from the operation interface of a member device to that of the management device | **cluster switch-to administrator** | Required |

**Caution**

Telnet connection is used in the switching between the management device and a member device. Note the following when switching between them:

- Authentication is required when you switch from a member device to the management device. The switching fails if authentication is not passed. Your user level is allocated according to the predefined level by the management device if authentication is passed.
- When a candidate device is added to a cluster and becomes a member device, its super password will be automatically synchronized to the management device. Therefore, after a cluster is established, it is not recommended to modify the super password of any member (including the management device and member devices) of the cluster; otherwise, the switching may fail because of an authentication failure.
- If the member specified in this command does not exist, the system prompts error when you execute the command; if the switching succeeds, your user level on the management device is retained.
- If the Telnet users on the device to be logged in reach the maximum number, the switching fails.
- To prevent resource waste, avoid ring switching when configuring access between cluster members. For example, if you switch from the operation interface of the management device to that of a member device and then need to switch back to that of the management device, use the **quit** command to end the switching, but not the **cluster switch-to administrator** command to switch to the operation interface of the management device.

## Adding a Candidate Device to a Cluster

Follow these steps to add a candidate device to a cluster:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Add a candidate device to the cluster | **administrator-address** *mac-address* **name** *name* | Required |

# Configuring Advanced Cluster Functions

This section covers these topics:

- Configuring Topology Management
- Configuring Interaction for a Cluster
- SNMP Configuration Synchronization Function
- Configuring Web User Accounts in Batches

## Configuring Topology Management

The concepts of blacklist and whitelist are used for topology management. An administrator can diagnose the network by comparing the current topology (namely, the information of a node and its neighbors in the cluster) and the standard topology.

- Topology management whitelist (standard topology): A whitelist is a list of topology information that has been confirmed by the administrator as correct. You can get the information of a node and its neighbors from the current topology. Based on the information, you can manage and maintain the whitelist by adding, deleting or modifying a node.
- Topology management blacklist: Devices in a blacklist are not allowed to join a cluster. A blacklist contains the MAC addresses of devices. If a blacklisted device is connected to a network through another device not included in the blacklist, the MAC address and access port of the latter are also included in the blacklist. The candidate devices in a blacklist can be added to a cluster only if the administrator manually removes them from the list.

The whitelist and blacklist are mutually exclusive. A whitelist member cannot be a blacklist member, and vice versa. However, a topology node can belong to neither the whitelist nor the blacklist. Nodes of this type are usually newly added nodes, whose identities are to be confirmed by the administrator.

You can back up and restore the whitelist in the following two ways:

- Backing them up on the FTP server shared by the cluster. You can manually restore the whitelist and blacklist from the FTP server.
- Backing them up in the Flash of the management device. When the management device restarts, the whitelist and blacklist will be automatically restored from the Flash. When a cluster is re-established, you can choose whether to restore the whitelist and blacklist from the Flash automatically, or you can manually restore them from the Flash of the management device.

Follow these steps to configure cluster topology management:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Add a device to the blacklist | **black-list add-mac** *mac-address* | Optional |
| Remove a device from the blacklist | **black-list delete-mac** { **all** \| *mac-address* } | Optional |

| To do… | Use the command… | Remarks |
|---|---|---|
| Confirm the current topology and save it as the standard topology | **topology accept** { **all** [ **save-to** { **ftp-server** \| **local-flash** } ] \| **mac-address** *mac-address* \| **member-id** *member-number* } | Optional |
| Save the standard topology to the FTP server or the local Flash | **topology save-to** { **ftp-server** \| **local-flash** } | Optional |
| Restore the standard topology information from the FTP server or the local Flash | **topology restore-from** { **ftp-server** \| **local-flash** } | Optional |

## Configuring Interaction for a Cluster

After establishing a cluster, you can configure FTP/TFTP server, NM host and log host for the cluster on the management device.

- After you configure an FTP/TFTP server for a cluster, the members in the cluster access the FTP/TFTP server configured through the management device.
- After you configure a log host for a cluster, all the log information of the members in the cluster will be output to the configured log host in the following way: first, the member devices send their log information to the management device, which then converts the addresses of log information and sends them to the log host.
- After you configure an NM host for a cluster, the member devices in the cluster send their Trap messages to the shared SNMP NM host through the management device.

If the port of an access NM device (including FTP/TFTP server, NM host and log host) does not allow the packets from the management VLAN to pass, the NM device cannot manage the devices in a cluster through the management device. In this case, on the management device, you need to configure the VLAN interface of the access NM device (including FTP/TFTP server, NM host and log host) as the NM interface.

Follow these steps to configure the interaction for a cluster:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure the FTP server shared by the cluster | **ftp-server** *ip-address* [ **user-name** *username* **password** { **simple** \| **cipher** } *password* ] | Required<br>By default, no FTP server is configured for a cluster. |
| Configure the TFTP server shared by the cluster | **tftp-server** *ip-address* | Required<br>By default, no TFTP server is configured for a cluster. |
| Configure the log host shared by the member devices in the cluster | **logging-host** *ip-address* | Required<br>By default, no log host is configured for a cluster. |
| Configure the SNMP NM host shared by the cluster | **snmp-host** *ip-address* [ **community-string read** *string1* **write** *string2* ] | Required<br>By default, no SNMP host is configured. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the NM interface of the management device | **nm-interface vlan-interface** *vlan-interface-id* | Optional |

**Caution**

To isolate management protocol packets of a cluster from packets outside the cluster, you are recommended to configure to prohibit packets from the management VLAN from passing the ports that connect the management device with the devices outside the cluster and configure the NM interface for the management device.

## SNMP Configuration Synchronization Function

SNMP configuration synchronization function facilitates management of a cluster, with which you can perform SNMP-related configurations on the management device and synchronize them to the member devices on the whitelist. This operation is equal to configuring multiple member devices at one time, simplifying the configuration process. Follow these steps to configure the SNMP configuration synchronization function:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure the SNMP community name shared by a cluster | **cluster-snmp-agent community** { **read** \| **write** } *community-name* [ **mib-view** *view-name* ] | Required |
| Configure the SNMPv3 group shared by a cluster | **cluster-snmp-agent group v3** *group-name* [ **authentication** \| **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] | Required |
| Create or update information of the MIB view shared by a cluster | **cluster-snmp-agent mib-view included** *view-name oid-tree* | Required<br>By default, the name of the MIB view shared by a cluster is ViewDefault and a cluster can access the ISO subtree. |
| Add a user for the SNMPv3 group shared by a cluster | **cluster-snmp-agent usm-user v3** *user-name group-name* [ **authentication-mode** { **md5** \| **sha** } *auth-password* ] [ **privacy-mode des56** *priv-password* ] | Required |

**Note**

- The SNMP-related configurations are retained when a cluster is dismissed or the member devices are removed from the whitelist.
- For information about SNMP, refer to *SNMP Configuration* in the *System Volume*.

## Configuring Web User Accounts in Batches

Configuring Web user accounts in batches enables you to configure on the management device the username and password used to log in to the devices (including the management device and member devices) within a cluster through Web and synchronize the configurations to the member devices in the whitelist. This operation is equal to performing the configurations on the member devices. You need to enter your username and password when you log in to the devices (including the management device and member devices) in a cluster through Web.

Follow these steps to configure Web user accounts in batches:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure Web user accounts in batches | **cluster-local-user** *username* **password** { **cipher** \| **simple** } *password* | Required |

**Note**

If a cluster is dismissed or the member devices are removed from the whitelist, the configurations of Web user accounts are still retained.

# Displaying and Maintaining Cluster Management

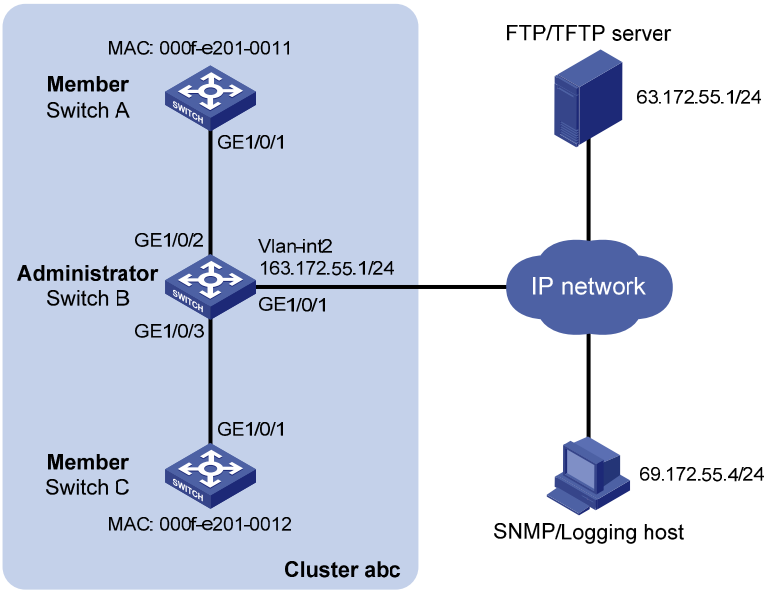
| To do… | Use the command… | Remarks |
|---|---|---|
| Display NDP configuration information | **display ndp** [ **interface** *interface-list* ] | Available in any view |
| Display the global NTDP information | **display ntdp** | |
| Display the device information collected through NTDP | **display ntdp device-list** [ **verbose** ] | |
| Display the detailed NTDP information of a specified device | **display ntdp single-device mac-address** *mac-address* | |
| View cluster state and statistics | **display cluster** | |
| View the standard topology information | **display cluster base-topology** [ **mac-address** *mac-address* \| **member-id** *member-number* ] | |
| View the current blacklist of the cluster | **display cluster black-list** | |
| View the information of candidate devices | **display cluster candidates** [ **mac-address** *mac-address* \| **verbose** ] | |
| Display the current topology information or the topology path between two devices | **display cluster current-topology** [ **mac-address** *mac-address* [ **to-mac-address** *mac-address* ] \| **member-id** *member-number* [ **to-member-id** *member-number* ] ] | |
| Display members in a cluster | **display cluster members** [ *member-number* \| **verbose** ] | |
| Clear NDP statistics | **reset ndp statistics** [ **interface** *interface-list* ] | Available in user view |

# Cluster Management Configuration Example

## Network requirements

- Three switches form cluster **abc**, whose management VLAN is VLAN 10. In the cluster, Switch B serves as the management device (Administrator), whose network management interface is VLAN-interface 2; Switch A and Switch C are the member devices (Member).
- All the devices in the cluster use the same FTP server and TFTP server on host 63.172.55.1/24, and use the same SNMP NMS and log services on host IP address: 69.172.55.4/24.
- Add the device whose MAC address is 000f-e201-0013 to the blacklist.

**Figure 1-4** Network diagram for cluster management configuration




## Configuration procedure

1) Configure the member device Switch A

# Enable NDP globally and for port GigabitEthernet 1/0/1.

```
<SwitchA> system-view
[SwitchA] ndp enable
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ndp enable
[SwitchA-GigabitEthernet1/0/1] quit
```

# Enable NTDP globally and for port GigabitEthernet 1/0/1.

```
[SwitchA] ntdp enable
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ntdp enable
[SwitchA-GigabitEthernet1/0/1] quit
```

# Enable the cluster function.

```
[SwitchA] cluster enable
```

2) Configure the member device Switch C

As the configurations of the member devices are the same, the configuration procedure of Switch C is omitted here.

3) Configure the management device Switch B

# Enable NDP globally and for ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
<SwitchB> system-view
[SwitchB] ndp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ndp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ndp enable
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

# Configure the period for the receiving device to keep NDP packets as 200 seconds.

```
[SwitchB] ndp timer aging 200
```

# Configure the interval to send NDP packets as 70 seconds.

```
[SwitchB] ndp timer hello 70
```

# Enable NTDP globally and for ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchB] ntdp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ntdp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ntdp enable
[SwitchB-GigabitEthernet1/0/3] quit
```

# Configure the hop count to collect topology as 2.

```
[SwitchB] ntdp hop 2
```

# Configure the delay to forward topology-collection request packets on the first port as 150 ms.

```
[SwitchB] ntdp timer hop-delay 150
```

# Configure the delay to forward topology-collection request packets on the first port as 15 ms.

```
[SwitchB] ntdp timer port-delay 15
```

# Configure the interval to collect topology information as 3 minutes.

```
[SwitchB] ntdp timer 3
```

# Configure the management VLAN of the cluster as VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] management-vlan 10
```

# Configure ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as Trunk ports and allow packets from the management VLAN to pass.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
```

# Enable the cluster function.

```
[SwitchB] cluster enable
```

# Configure a private IP address range for the member devices, which is from 172.16.0.1 to 172.16.0.7.

```
[SwitchB] cluster
[SwitchB-cluster] ip-pool 172.16.0.1 255.255.255.248
```

# Configure the current device as the management device, and establish a cluster named **abc**.

```
[SwitchB-cluster] build abc
```

```
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
N
```

# Enable management VLAN auto-negotiation.

```
[abc_0.SwitchB-cluster] management-vlan synchronization enable
```

# Configure the holdtime of the member device information as 100 seconds.

```
[abc_0.SwitchB-cluster] holdtime 100
```

# Configure the interval to send handshake packets as 10 seconds.

```
[abc_0.SwitchB-cluster] timer 10
```

# Configure the FTP Server, TFTP Server, Log host and SNMP host for the cluster.

```
[abc_0.SwitchB-cluster] ftp-server 63.172.55.1
[abc_0.SwitchB-cluster] tftp-server 63.172.55.1
[abc_0.SwitchB-cluster] logging-host 69.172.55.4
[abc_0.SwitchB-cluster] snmp-host 69.172.55.4
```

# Add the device whose MAC address is 00E0-FC01-0013 to the blacklist.

```
[abc_0.SwitchB-cluster] black-list add-mac 00e0-fc01-0013
[abc_0.SwitchB-cluster] quit
```

# Add port GigabitEthernet 1/0/1 to VLAN 2, and configure the IP address of VLAN-interface 2.

```
[abc_0.SwitchB] vlan 2
[abc_0.SwitchB-vlan2] port gigabitethernet 1/0/1
[abc_0.SwitchB] quit
[abc_0.SwitchB] interface vlan-interface 2
[abc_0.SwitchB-Vlan-interface2] ip address 163.172.55.1 24
[abc_0.SwitchB-Vlan-interface2] quit
```

# Configure VLAN-interface 2 as the network management interface.

```
[abc_0.SwitchB] cluster
[abc_0.SwitchB-cluster] nm-interface vlan-interface 2
```

# Table of Contents

# 1 Stack Configuration

When configuring stack, go to these sections for information you are interested in:



## Stack Configuration Overview

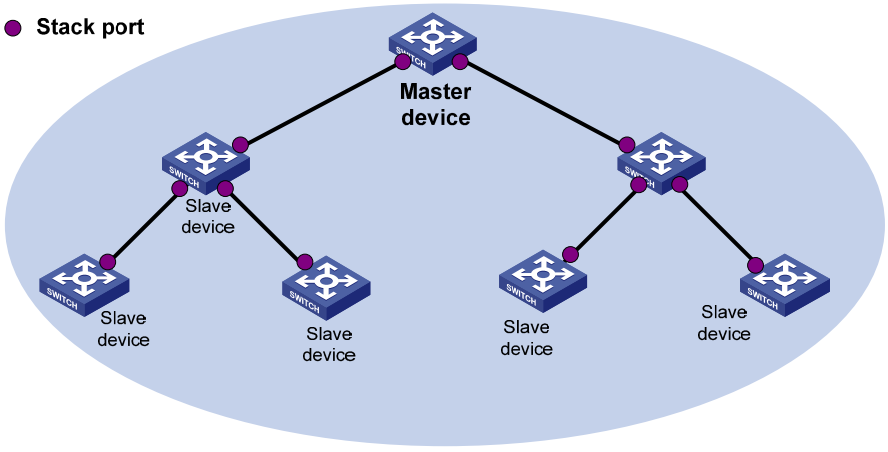
A stack is a set of network devices. Administrators can group multiple network devices into a stack and manage them as a whole. Therefore, stack management can help reduce customer investments and simplify network management.

### Introduction to Stack

A stack is a management domain that comprises several network devices connected to one another through stack ports. In a stack, there is a master device and several slave devices.

An administrator can manage all the devices in a stack through the master device. Figure 1-1 shows a network diagram for stack management.

**Figure 1-1** Network diagram for stack management




- Master device: In a stack, the master device acts as the configuration interface in stack management. Management and monitoring of all the devices in the stack are performed through the master device.
- Slave devices: Managed devices in a stack.
- Stack port: Ports between stack devices.

### Establishing a Stack

An administrator can establish a stack as follows:

- Configure a private IP address pool for a stack and create the stack on the network device which is desired to be the master device.
- Configure ports between the stack devices as stack ports.
- The master device automatically adds the slave devices into the stack, and assigns a number for each stack member.
- The administrator can log in to any slave device from the master device of the stack, and perform configurations for the slave device.

## Stack Configuration Task List

Complete the following tasks to configure stack:

| Task | | Remarks |
|---|---|---|
| Configuring the Master Device of a Stack | Configuring a Private IP Address Pool for a Stack | Required |
| | Configuring Stack Ports | Required |
| | Creating a Stack | Required |
| Configuring Stack Ports of a Slave Device | | Required |
| Logging In to the CLI of a Slave from the Master | | Optional |

## Configuring the Master Device of a Stack

### Configuring a Private IP Address Pool for a Stack

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a private IP address pool for the stack | **stack ip-pool** *ip-address* { *mask* \| *mask-length* } | Required<br>By default, no IP address pool is configured for a stack. |

**Note**

- If a device is already configured as the master device of a stack or is already a slave device of a stack, you cannot configure a private IP address pool on the device.
- When you configure a private IP address pool for a stack, the number of IP addresses in the address pool needs to be equal to or greater than the number of devices to be added to the stack. Otherwise, some devices may not be able to join the stack automatically for lack of private IP addresses.

### Configuring Stack Ports

On the master device, configure ports that connect to slave devices as stack ports.

Follow the steps below to configure stack ports:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified ports as stack ports | **stack stack-port** *stack-port-num* **port** *interface-list* | Required<br>By default, a port is not a stack port. |

### Creating a Stack

After you execute the **stack role master** command on a stack-capable device, the device becomes the master device of a stack and automatically adds the devices connected with its stack ports to the stack.

Follow the steps below to create a stack:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a stack | **stack role master** | Required |

**Note**

After you configure a device as the master device of a stack, the prompt changes to <stack_0.Sysname>, where Sysname is the system name of the device.

## Configuring Stack Ports of a Slave Device

You need to configure stack ports to add a slave device to the stack.

The ports of a slave device that connect to other stack devices need to be configured as stack ports.

Follow the steps below to configure stack ports:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the specified ports as stack ports | **stack stack-port** *stack-port-num* **port** *interface-list* | Required<br>By default, a port is not a stack port. |

**Note**

After a device joins a stack and becomes a slave device of the stack, the prompt changes to <stack_n.Sysname>, where n is the stack number assigned by the master device, and Sysname is the system name of the device.

## Logging In to the CLI of a Slave from the Master

In a stack, you can log in to the CLI of a slave device from the master device and perform configurations for the slave device.

Follow the step below to log in to the CLI of a slave device from the master device:

| To do… | Use the command… | Remarks |
|---|---|---|
| Log in to the CLI of the specified slave device from the master device | **stack switch-to** *member-id* | Required<br>Available in user view |

**Note**

The **stack switch-to** command is used to log in to the CLI of a slave device from the master with the user level being unchanged. To return to the master device, use the **quit** command.

## Displaying and Maintaining Stack Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the stack information of stack members | **display stack** [ **members** ] | Available in any view |

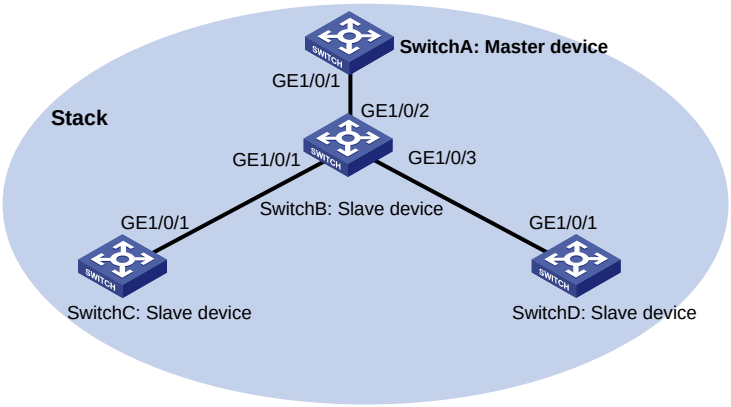
## Stack Configuration Example

### Stack Configuration Example

#### Network requirements

- Switch A, Switch B, Switch C, and Switch D are connected with one another.
- Create a stack, where Switch A is the master device, Switch B, Switch C, and Switch D are slave devices. An administrator can log in to Switch B, Switch C and Switch D through Switch A to perform remote configurations.

**Figure 1-2** Network diagram for stack management




## Configuration procedure

1) Configure the master device

# Configure a private IP address pool for the stack on Switch A.

```
<SwitchA> system-view
[SwitchA] stack ip-pool 192.168.1.1 24
```

# Configure port GigabitEthernet 1/0/1 as a stack port on Switch A.

```
[SwitchA] stack stack-port 1 port GigabitEthernet 1/0/1
```

# Configure switch A as the master device.

```
[SwitchA] stack role master
```

2) Configure the slave devices

# On Switch B, configure local ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/1, and GigabitEthernet 1/0/3 as stack ports.

```
<SwitchB> system-view
[SwitchB] stack stack-port 3 port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
GigabitEthernet 1/0/3
```

# On Switch C, configure local port GigabitEthernet 1/0/1 as a stack port.

```
<SwitchC> system-view
[SwitchC] stack stack-port 1 port GigabitEthernet 1/0/1
```

# On Switch D, configure local port GigabitEthernet 1/0/1 as a stack port.

```
<SwitchD> system-view
[SwitchD] stack stack-port 1 port GigabitEthernet 1/0/1
```

3) Verify the configuration

# Display stack information of the stack members on Switch A.

```
<stack_0.SwitchA> display stack members
Number     : 0
Role       : Master
Sysname    : stack_0. SwitchA
Switch type: Switch 4500G 24-Port
MAC address: 000f-e200-1000
```

```
Number     : 1
Role       : Slave
Sysname    : stack_1. SwitchB
Device type: Switch 4500G 24-Port
MAC address: 000f-e200-1001

Number     : 2
Role       : Slave
Sysname    : stack_2. DeviceC
Device type: Switch 4500G 24-Port
MAC address: 000f-e200-1002

Number     : 3
Role       : Slave
Sysname    : stack_3. DeviceD
Device type: Switch 4500G 24-Port
MAC address: 000f-e200-1003
```

# Table of Contents

# 1 Automatic Configuration

When configuring automatic configuration, go to these sections for information you are interested in:

- Introduction to Automatic Configuration
- Typical Networking of Automatic Configuration
- How Automatic Configuration Works

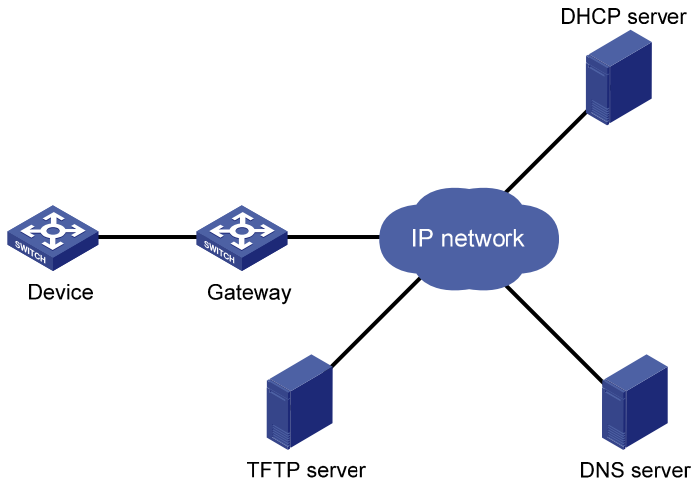
## Introduction to Automatic Configuration

Automatic configuration enables a device to automatically obtain and execute the configuration file when it starts up without loading the configuration file.

Automatic configuration simplifies network configuration, facilitating centralized management of devices. Currently, enterprise networks are facing the problems of large distribution of devices and less administrators, resulting in the huge cost for administrators to manually configure each device. With the automatic configuration function, network administrators can save the configuration files on a specified server and the device can automatically obtain and execute the configuration files, therefore greatly reducing the workload of administrators.

## Typical Networking of Automatic Configuration

**Figure 1-1** Network diagram for automatic configuration




As shown in Figure 1-1, the device implements automatic configuration with the cooperation of a DHCP server, TFTP server and DNS server:

- DHCP server: Assigns an IP address, configure file name, TFTP server IP address, and DNS server IP address for the device that performs automatic configuration.
- TFTP server: Saves files needed in automatic configuration. A device obtains files needed from a TFTP server, for example, network intermediate file and the configuration file of the device.
- DNS server: Used for IP address-to-host name resolution. A device that performs automatic configuration can resolve an IP address to a host name through a DNS server to get the configuration file with the name **hostname.cfg** from a TFTP server; if the device gets the domain

name of the TFTP server from a DHCP response, the device can also resolve the domain name of the TFTP server to the IP address of the TFTP server through the DNS server.

If the DHCP server, TFTP server, DNS server, and the device that performs automatic configuration are not in the same segment, you need to configure DHCP relay on a device working as a gateway.

# How Automatic Configuration Works

Basically, automatic configuration works in the following ways:

1) When a device starts up without loading any configuration file, the system sets the first active interface (if an active Layer 2 Ethernet interface exists, this first interface is a virtual interface corresponding with the default VLAN) as the DHCP client to request from the DHCP server for parameters, such as an IP address and name of a TFTP server, IP address of a DNS server, and the configuration file name.
2) After getting related parameters, the device will send a TFTP request to obtain the configuration file from the specified TFTP server for system initialization. If the client cannot get such parameters, it performs system initialization without loading any configuration file.

---

**Note**

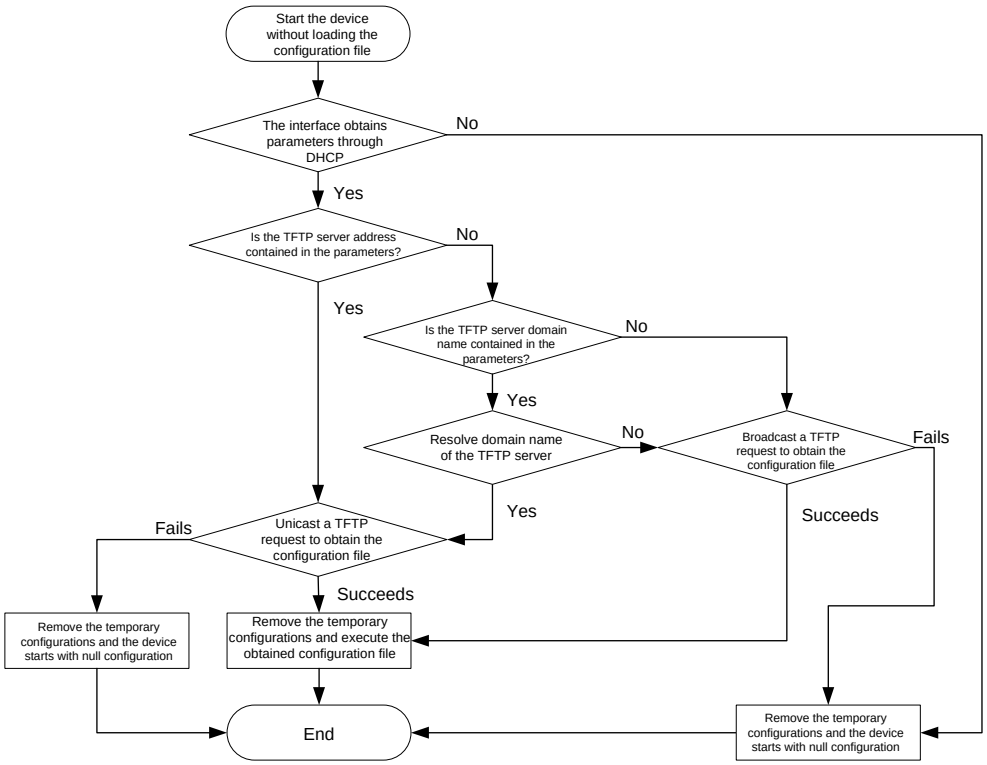
- To implement auto-configuration, you need to configure some parameters on the DHCP server, DNS server and TFTP server, but you do not need to perform any configuration on the device that starts up without loading any configuration file. The configuration mode depends on the device model; it is omitted here.
- If you need to use the automatic configuration function, you are recommended to connect only the interfaces needed in automatic configuration to the network.

---

## Work Flow of Automatic Configuration

The work flow of automatic configuration is as shown in Figure 1-2.

**Figure 1-2** Work flow of automatic configuration




## Obtaining the IP Address of an Interface and Related Information Through DHCP

### Obtaining an IP address

When a device starts up without loading the configuration file, the system automatically configures the first active interface (if an active Layer 2 Ethernet interface exists, this first interface is a virtual interface corresponding with the default VLAN) of the device as obtaining its IP address through DHCP. The device broadcasts a DHCP request through this interface. The Option 55 field specifies the information (for example, the configuration file name, domain name and IP address of the TFTP server and DNS server needed for obtaining the automatic configuration files) that the device can obtain from the DHCP server.

Upon successfully obtaining its IP address through DHCP, the device resolves the Option 67 (or the file field, configuration file name) field, Option 66 (domain name of the TFTP server) field, Option 150 (IP address of the TFTP server) field and Option 6 (IP address of the DNS server) field. If failing to obtain its IP address, the device removes the temporary configuration and starts up without loading the configuration file.

**Note**

- The configuration file name is saved in the Option 67 or file field of the DHCP response. The device first resolves the Option 67 field; if this field contains the configuration file name, the device does not resolve the file field; otherwise, it resolves the file field.
- Temporary configuration contains two parts: the configuration on the interface where automatic configuration is performed when the device starts up with default configuration; and the executed **ip host** command when the device is resolving the network intermediate file (For the detailed description of the **ip host** command, refer to *Domain Name Resolution Commands* in the *IP Services Volume.*). Removal of the temporary configuration is to execute the **undo** commands.
- For the detailed introduction to DHCP, refer to *DHCP Configuration* in the *IP Services Volume.*

### Principles for selecting an address pool on the DHCP server

The DHCP server selects IP addresses and other network configuration parameters from an address pool when assigning an IP address to a client. DHCP supports two mechanisms for IP address allocation.

- Dynamic address allocation: The DHCP server assigns an IP address and other configuration parameters in an address pool to a client.
- Manual address allocation: The DHCP server will select an address pool where an IP address is statically bound to the MAC address or ID of the client and assign the statically bound IP address and other configuration parameters to the client.

You can configure an address allocation mode as needed:

- Different devices with the same configuration file: You can configure dynamic address allocation on the DHCP server to assign IP addresses and the same configuration parameters (for example, configuration file name) to the devices. If this address allocation mode is adopted, the configuration file can only contain common configurations of the devices, and the specific configurations of each device need to be performed in other ways. For example, you need to specify to enable Telnet on a device through the configuration file obtained in automatic configuration and create a local user to facilitate the administrator to Telnet to each device to perform specific configurations (for example, configure the IP address of each interface).
- Different devices with different configuration files: You need to configure an address pool where an IP address is statically bound to the MAC address or ID of the client, to ensure that a specific client can be assigned with a fixed IP address and other configuration parameters. Through this address allocation mode, you can specify different configuration commands for each device, without the need to configure the device through other modes.

**Note**

You need to configure a client ID (when a device works as the DHCP client, it uses the client ID as its ID) of the static binding when you configure manual address allocation. Therefore, you need to obtain the client ID in this way: start the device that performs automatic configuration, enable the interface that performs automatic configuration to obtain its IP address through DHCP, after the IP address is successfully obtained, use the **display dhcp server ip-in-use** command to display address binding information on the DHCP server, thus to obtain the client ID of the device.

## Obtaining the Configuration File from the TFTP Server

### Configuration file type

The device can obtain the following types of configuration file from the TFTP server with the automatic configuration function enabled:

- The configuration file specified by the Option 67 or file field in the DHCP response
- The intermediate file, with the file name as **network.cfg**, used to save the mapping between the IP address and the host name. The mapping is defined in the following format:

**ip host** *hostname ip-address*

For example, the intermediate file can include the following:

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

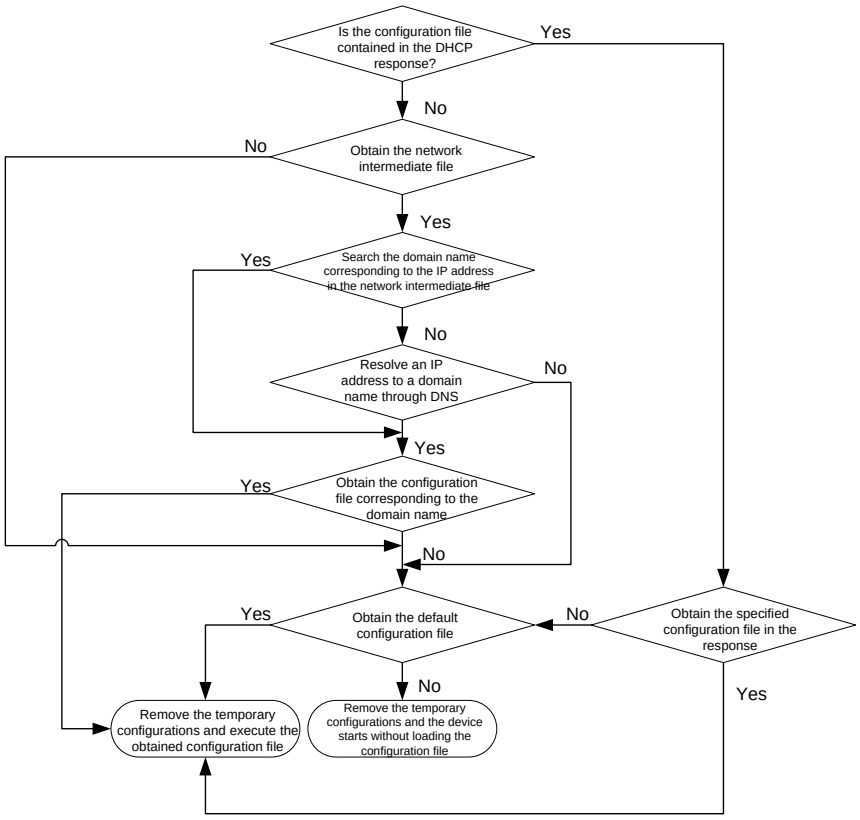
**Caution**

- There must be a space before the keyword **ip host**.
- The host name saved in the intermediate file must be the same with the configuration file name of the host. This host name is not the one saved in the DNS server, and their names can be the same or different.

- The configuration file corresponding with the host name of the device, with its file name as **hostname.cfg**. For example, if the host name of the device is **aaa**, then the configuration file name is **aaa.cfg**.
- Default configuration file, with the name as **device.cfg**.

## Obtaining the configuration file

**Figure 1-3** Obtain the configuration file




The device obtains the configuration file from the TFTP server based on its resolution of the configuration file name in the DHCP response:

- If the DHCP response contains information such as configuration file name, the device requests the specified configuration file from the TFTP server.
- If no information such as configuration file name is contained in the DHCP response, the device should obtain its host name first and then requests the configuration file corresponding with the host name. The device can obtain its host name in two steps: obtaining the intermediate file from the TFTP server and then searching in the intermediated file for its host name corresponding with the IP address of the device; if fails, the device obtains the host name from the DNS server.
- If the device fails to obtain the specified configuration file and resolve its host name or fails to obtain the configuration file corresponding with the host name, it requests the default configuration file from the TFTP server.

## Sending mode of a TFTP request

The device selects the sending mode of the TFTP request based on its resolution of the TFTP server's domain name and IP address in the DHCP response:

- If a legitimate TFTP server IP address is contained in the DHCP response, the device unicasts a TFTP request to the TFTP server and does not resolve the domain name of the TFTP server. Otherwise, the device resolves the TFTP domain name.
- If a legitimate TFTP server domain name is contained in the DHCP response, the device resolves the IP address of the TFTP server through DNS server. If succeeds, the device unicasts a TFTP request to the TFTP server; if fails, the device broadcasts a TFTP request to the TFTP server.

- If the IP address and the domain name of the TFTP server are not contained in the DHCP response or they are illegitimate, the device broadcasts a TFTP request to the TFTP server.

---

 **Note**

- When broadcasting a TFTP request, the device obtains the configuration file from the TFTP server who responds the first. If the required configuration file does not exist on the TFTP server, then obtaining the configuration file fails, and the device removes the temporary configuration and starts up without loading the configuration file.
- When the device broadcasts a TFTP request to the TFTP server, you need to configure the UDP Helper function on a gateway to transfer broadcasts to unicasts and forwards the unicasts to the specified TFTP server if the device performs the automatic configuration and the TFTP server are not in the same segment because broadcasts can only be transmitted in a segment. For the detailed description of the UDP Helper function, refer to *UDP Helper Configuration* in the *IP Services Volume*.

---

## Executing the Configuration File

Upon successfully obtaining the configuration file, the device removes the temporary configuration and executes the obtained configuration file; otherwise, it removes the temporary configuration and starts up without loading the configuration file.

---

 **Note**

After the device executes the configuration file obtained, the configuration file will be deleted. Therefore, you are recommended to save the configuration using the **save** command; otherwise, the device needs to perform the automatic configuration function after system reboot. For the detailed description of the **save** command, refer to *File System Management Configuration* in the *System Volume*.

---