3Com® Switch 5500 Family
Configuration Guide

Switch 5500-EI
Switch 5500G-EI
CONTENTS

ABOUT THIS GUIDE
Conventions 17
Related Documentation 18

1 CLI CONFIGURATION
Introduction to the CLI 19
Command Hierarchy 19
CLI Views 24
CLI Features 27

2 LOGGING INTO AN ETHERNET SWITCH
Logging into an Ethernet Switch 31
Introduction to the User Interface 31

3 LOGGING IN THROUGH THE CONSOLE PORT
Introduction 35
Logging In Through the Console Port 35
Console Port Login Configuration 38
Console Port Login Configuration with Authentication Mode Being None 39
Console Port Login Configuration with Authentication Mode Being Password 43
Console Port Login Configuration with Authentication Mode Being Scheme 46

4 LOGGING IN THROUGH TELNET
Introduction 51
Telnet Configuration with Authentication Mode Being None 53
Configuring Telnet with the Password Authentication Mode 55
Telnet Configuration with Authentication Mode Being Scheme 58
Using Telnet to Connect to a Switch 62

5 LOGGING IN USING A MODEM
Introduction 67
Configuration on the Switch Side 67
Modem Connection Establishment 68
6 LOGGING IN THROUGH THE WEB-BASED NETWORK MANAGEMENT SYSTEM
   Introduction 71
   Establishing an HTTP Connection 71
   Configuring the Login Banner 72
   Enabling/Disabling the WEB Server 73

7 LOGGING IN THROUGH NMS
   Introduction 75
   Connection Establishment Using NMS 75

8 CONFIGURING SOURCE IP ADDRESSES FOR TELNET SERVICE PACKETS
   Overview 77
   Configuring a Source IP Address for Telnet Service Packets 77
   Displaying the Source IP Address Configuration 78

9 USER CONTROL
   Introduction 79
   Controlling Telnet Users 79
   Controlling Network Management Users by Source IP Addresses 81
   Controlling Web Users by Source IP Address 83

10 CONFIGURATION FILE MANAGEMENT
   Introduction to the Configuration File 87
   Management of Configuration File 88

11 XRN CONFIGURATION
   Introduction to XRN 93
   Configuring an XRN Fabric 94
   Fabric Configuration Example 97
   RMON on XRN 98
   Clustering on XRN 98
   Peer Fabric Port Detection 99
   Multiple Fabric Port Candidates 101

12 VLAN OVERVIEW
   VLAN Overview 103
   Port-Based VLAN 106
   Protocol-Based VLAN 108

13 VLAN CONFIGURATION
   VLAN Configuration 113
   Configuring a Port-Based VLAN 114
21 **PORT SECURITY CONFIGURATION**
Port Security Overview 185
Port Security Configuration 188
Displaying and Maintaining Port Security Configuration 193
Port Security Configuration Example 193

22 **PORT BINDING CONFIGURATION**
Port Binding Overview 195
Displaying Port Binding Configuration 195
Port Binding Configuration Example 196

23 **DLDP CONFIGURATION**
Overview 197
DLDP Configuration 204
DLDP Configuration Example 206

24 **MAC ADDRESS TABLE MANAGEMENT**
Introduction to the MAC Address Table 210
Managing the MAC Address Table 212
Configuring MAC Address Table Management 213
Displaying MAC Address Table Information 217
Configuration Example 217

25 **AUTO DETECT CONFIGURATION**
Introduction to the Auto Detect Function 219
Auto Detect Configuration 219
Auto Detect Configuration Example 222

26 **MSTP CONFIGURATION**
STP Overview 227
MSTP Overview 235
Configuring Root Bridge 241
Configuring Leaf Nodes 255
Performing mCheck Operation 259
Configuring Guard Functions 260
Configuring Digest Snooping 264
Configuring Rapid Transition 266
Configuring VLAN-VPN Tunnel 268
STP Maintenance Configuration 270
Enabling Trap Messages Conforming to 802.1d Standard 270
Displaying and Maintaining MSTP 271
MSTP Configuration Example 271
VLAN-VPN tunnel Configuration Example 273
## 32 IP ROUTING POLICY CONFIGURATION
- IP Routing Policy Overview 369
- IP Routing Policy Configuration Tasks 370
- Routing Policy Configuration 371
- AS Path List Configuration 373
- Community List Configuration 373
- IP-Prefix Configuration 374
- Displaying IP Routing Policy 375
- IP Routing Policy Configuration Example 375
- Troubleshooting IP Routing Policy 381

## 33 ROUTE CAPACITY CONFIGURATION
- Route Capacity Configuration Overview 383
- Route Capacity Limitation Configuration 384
- Displaying and Maintaining Route Capacity Limitation Configuration 384

## 34 MULTICAST OVERVIEW
- Multicast Overview 385
- Multicast Models 389
- Multicast Architecture 389
- Multicast Packet Forwarding Mechanism 394

## 35 COMMON MULTICAST CONFIGURATION
- Common Multicast Configuration 397
- Displaying and Maintaining Common Multicast Configuration 400

## 36 IGMP CONFIGURATION
- IGMP Overview 403
- Configuring IGMP 407
- Displaying IGMP 412

## 37 PIM CONFIGURATION
- PIM Overview 413
- Configuring PIM-DM 421
- Configuring PIM-SM 422
- Displaying PIM 426
- Configuring Common PIM Parameters 427
- Displaying and Maintaining PIM 430
- PIM Configuration Examples 430
- Troubleshooting PIM 437

## 38 MSDP CONFIGURATION
- MSTP Overview 439
- Configuring MSDP Basic Functions 445
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
</table>

| 10       |

| RADIUS Configuration Task List | 527 |
| HWTACACS Configuration Task List | 537 |
| Displaying and Maintaining AAA Configuration | 541 |
| AAA Configuration Examples | 543 |
| Troubleshooting AAA | 547 |

### 46 EAD Configuration

| Introduction to EAD | 549 |
| Typical Network Application of EAD | 549 |
| Configuring EAD | 550 |
| EAD Configuration Example | 551 |

### 47 VRRP Configuration

| VRRP Overview | 553 |
| VRRP Configuration | 559 |
| Displaying and Maintaining VRRP | 561 |
| VRRP Configuration Examples | 561 |
| Troubleshooting VRRP | 570 |

### 48 MAC Address Authentication Configuration

| MAC Address Authentication Overview | 571 |
| Related Concepts | 572 |
| Configuring Basic MAC Address Authentication Functions | 572 |
| MAC Address Authentication Enhanced Function Configuration | 573 |
| Displaying and Maintaining MAC Address Authentication | 576 |
| MAC Address Authentication Configuration Example | 576 |

### 49 ARP Configuration

| Introduction to ARP | 579 |
| Configuring ARP | 584 |
| Configuring Gratuitous ARP | 586 |
| Displaying and Debugging ARP | 587 |
| ARP Configuration Example | 587 |

### 50 Proxy ARP Configuration

| Proxy ARP Overview | 591 |
| Configuring Proxy ARP | 592 |
| Proxy ARP Configuration Example | 592 |

### 51 Resilient ARP Configuration

| Resilient ARP Introduction | 595 |
| Configuring Resilient ARP | 595 |
| Resilient ARP Configuration Example | 596 |
## 52 DHCP OVERVIEW

- DHCP Introduction 597
- DHCP IP Address Assignment 597
- DHCP Packet Format 599
- Protocol Specification 600

## 53 DHCP SERVER CONFIGURATION

- Introduction to DHCP Server 601
- DHCP Server Configuration Task List 604
- Enabling DHCP 604
- Configuring the Global Address Pool Based DHCP Server 605
- Configuring the Interface Address Pool Based DHCP Server 614
- Configuring DHCP Server Security Functions 623
- Configuring DHCP Accounting Functions 624
- Enabling the DHCP Server to Process Option 82 625
- Displaying and Maintaining the DHCP Server 626
- DHCP Server Configuration Examples 626
- Troubleshooting a DHCP Server 631

## 54 DHCP RELAY AGENT CONFIGURATION

- Introduction to DHCP Relay Agent 633
- Configuring the DHCP Relay Agent 635
- Displaying and Maintaining DHCP Relay Agent Configuration 639
- DHCP Relay Agent Configuration Example 639
- Troubleshooting DHCP Relay Agent Configuration 640

## 55 DHCP SNOOPING CONFIGURATION

- Introduction to DHCP Snooping 643
- DHCP Snooping Configuration 647
- DHCP Snooping Configuration Example 651
- Displaying DHCP Snooping Configuration 653

## 56 DHCP PACKET RATE LIMIT CONFIGURATION

- Introduction to DHCP Packet Rate Limit 655
- Configuring DHCP Packet Rate Limit 655
- Rate Limit Configuration Example 656

## 57 DHCP/BOOTP CLIENT CONFIGURATION

- Introduction to the DHCP Client 659
- Introduction to BOOTP Client 659
- Configuring a DHCP/BOOTP Client 659
- Displaying DHCP/BOOTP Client Configuration 661
58 ACL CONFIGURATION
ACL Overview 663
ACL Configuration 665
Examples for Upper-layer Software Referencing ACLs 673
Example for Applying ACLs to Hardware 675

59 QoS CONFIGURATION
Overview 681
QoS Supported By Switch 5500 Family 682
QoS Configuration 693
QoS Configuration Example 705

60 QoS PROFILE CONFIGURATION
Overview 709
QoS Profile Configuration 710
Configuration Example 712

61 WEB CACHE REDIRECTION CONFIGURATION
Web Cache Redirection Overview 715
Web Cache Redirection Configuration 716
Displaying Web Cache Redirection Configuration 717
Web Cache Redirection Configuration Example 717

62 MIRRORING CONFIGURATION
Mirroring Overview 721
Configuring Mirroring 723
Mirroring Configuration Examples 727

63 IRF FABRIC CONFIGURATION
Introduction to IRF 733
An IRF Fabric on the Switch 5500 733
Configuring an IRF Fabric Configuration on the Switch 5500 738
Displaying and Maintaining IRF Fabric for the Switch 5500 742
Switch 5500 IRF Fabric Configuration Example 743
An IRF Fabric on the Switch 5500G 744
Configuring an IRF Fabric Configuration on the Switch 5500G 749
Displaying and Maintaining IRF Fabric for the Switch 5500G 752
Switch 5500G IRF Fabric Configuration Example 753

64 CLUSTERING
Cluster Overview 755
Cluster Configuration Tasks 763
Displaying and Maintaining Cluster Configuration 772
Cluster Configuration Examples 772
72  **FILE SYSTEM MANAGEMENT CONFIGURATION**
    File System Configuration  867
    File Attribute Configuration  870
    Configuration File Backup and Restoration  873

73  **FTP AND SFTP CONFIGURATION**
    Introduction to FTP and SFTP  875
    FTP Configuration  876
    SFTP Configuration  887

74  **TFTP CONFIGURATION**
    Introduction to TFTP  895
    TFTP Configuration  896

75  **INFORMATION CENTER**
    Information Center Overview  899
    Information Center Configuration  904
    Displaying and Maintaining Information Center  910
    Information Center Configuration Examples  910

76  **BOOT ROM AND HOST SOFTWARE LOADING**
    Introduction to Loading Approaches  915
    Local Boot ROM and Software Loading  915
    Remote Boot ROM and Software Loading  924

77  **BASIC SYSTEM CONFIGURATION AND DEBUGGING**
    Basic System Configuration  929
    Displaying the System Status  930
    Debugging the System  930

78  **NETWORK CONNECTIVITY TEST**
    Network Connectivity Test  933

79  **DEVICE MANAGEMENT**
    Introduction to Device Management  935
    Device Management Configuration  935
    Displaying the Device Management Configuration  938
    Remote Switch APP Upgrade Configuration Example  939
80 VLAN-VPN Configuration

VLAN-VPN Overview 943
VLAN-VPN Configuration 945
Displaying and Maintaining the VLAN-VPN Configuration 947
VLAN-VPN Configuration Example 947

81 Selective QinQ Configuration

Selective QinQ Overview 951
Selective QinQ Configuration 953
Selective QinQ Configuration Example 954

82 BPDU Tunnel Configuration

BPDU Tunnel Overview 959
BPDU Tunnel Configuration 961
Displaying BPDU Tunnel Configuration 962
BPDU Tunnel Configuration Example 962

83 Remote-ping Configuration

Remote-ping Overview 965
Remote-ping Configuration 968
Remote-ping Configuration Example 981

84 IPv6 Configuration

IPv6 Overview 995
IPv6 Configuration Task List 1002
IPv6 Configuration Example 1009

85 IPv6 Application Configuration

Introduction to IPv6 Application 1013
Configuring IPv6 Application 1013
IPv6 Application Configuration Example 1016
Troubleshooting IPv6 Application 1017

86 DNS Configuration

DNS Overview 1019
Configuring Domain Name Resolution 1021
Displaying and Maintaining DNS 1021
DNS Configuration Examples 1022
Troubleshooting DNS 1024

87 Smart Link Configuration

Smart Link Overview 1025
Configuring Smart Link 1027
Displaying and Maintaining Smart Link 1030
Smart Link Configuration Example 1030

88 **Monitor Link Configuration**
Introduction to Monitor Link 1033
Configuring Monitor Link 1034
Displaying Monitor Link Configuration 1036
Monitor Link Configuration Example 1036

89 **Access Management Configuration**
Access Management Overview 1039
Configuring Access Management 1040
Access Management Configuration Examples 1040

90 **Web Authentication Configuration**
Introduction to Web Authentication 1045
Web Authentication Configuration 1045
Displaying and Maintaining Web Authentication 1047
Web Authentication Configuration Example 1047
ABOUT THIS GUIDE

This guide describes the 3Com® Switch 5500 and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

This guide is intended for Qualified Service personnel who are responsible for configuring, using, and managing the switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.

Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation:

http://www.3com.com

Table 1 lists icon conventions that are used throughout this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Information note</td>
<td>Information that describes important features or instructions.</td>
</tr>
<tr>
<td>!</td>
<td>Caution</td>
<td>Information that alerts you to potential loss of data or potential damage to an application, system, or device.</td>
</tr>
<tr>
<td>!</td>
<td>Warning</td>
<td>Information that alerts you to potential personal injury.</td>
</tr>
</tbody>
</table>

Table 2 lists text conventions that are used throughout this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen displays</td>
<td>This typeface represents information as it appears on the screen.</td>
</tr>
<tr>
<td>Keyboard key names</td>
<td>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del</td>
</tr>
<tr>
<td>The words “enter” and “type”</td>
<td>When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”</td>
</tr>
</tbody>
</table>
The following manuals offer additional information necessary for managing your Switch 5500:

- **Switch 5500 Command Reference Guide** — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch 5500.

- **Switch 5500 Getting Started Guide**— Describes how to install your Switch 5500 or Switch 5500G.

- **Switch 5500 Release Notes** — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the Release Notes.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site:

http://www.3com.com/
Introduction to the CLI

A command line interface (CLI) is a user interface to interact with a switch. Through the CLI on a switch, you can enter commands to configure the switch and check output information to verify the configuration. Each Switch 5500 provides an easy-to-use CLI and a set of configuration commands for configuring and managing your switch.

The CLI on the Switch 5500 Family provides the following features:

- **Hierarchical command protection**: You can control the commands that specific users can execute to prevent unauthorized users from configuring the switch.
- **Online help**: Users can gain online help at any time by entering a question mark (?) at the command line prompt.
- **Debugging**: Detailed debugging information is provided to help diagnose and locate network problems.
- **Command history function**: This feature enables users to check most recently executed commands and makes it easier to execute those commands again.
- **Partial matching of commands**: The system allows you to enter partially matching text to search for commands. This allows you to execute a command by entering partially-spelled command keywords as long as the system can uniquely identify the keywords entered.

Command Hierarchy

The Switch 5500 uses hierarchical command protection for command lines, to prevent users with fewer access rights from using higher-level commands to change the switch’s configuration. Based on user privilege, commands are classified in four levels:

- **Visitor level (level 0)**: Commands at this level are mainly used to diagnose the network, and cannot be saved in a configuration file. For example, **ping**, **tracert**, and **telnet** are level 0 commands.
- **Monitor level (level 1)**: Commands at this level are mainly used to maintain the system and diagnose service faults. They cannot be saved in a configuration file. Such commands include **debugging** and **terminal**.
- **System level (level 2)**: Commands at this level are mainly used to configure services and include routing and network layer commands. These commands can be used to provide network services directly.
- **Manage level (level 3)**: Commands at this level are associated with the basic operation and support modules of the system. These commands provide
support for services. Commands concerning file system, FTP/TFTP/XModem downloading, user management, and level setting are at this level.

By default, the Console user (a user who logs into the switch through the Console port) is a level-3 user and Telnet users are level-0 users.

**User Level Switching**

<table>
<thead>
<tr>
<th>Table 1</th>
<th>User level switching configuration task list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Remarks</td>
</tr>
<tr>
<td>“Specifying the authentication mode for user level switching”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Adopting super password authentication for user level switching”</td>
<td>Required</td>
</tr>
<tr>
<td>“Adopting HWTACACS authentication for user level switching”</td>
<td>Required</td>
</tr>
<tr>
<td>“Switching to a specific user level”</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Specifying the authentication mode for user level switching**

You can switch between user levels through corresponding commands after logging into a switch successfully. The high-to-low user level switching is unlimited. However, the low-to-high user level switching requires the corresponding authentication. The super password authentication mode and HWTACACS authentication mode are available at the same time to provide authentication redundancy.

The configuration of authentication mode for user level switching is performed by Level-3 users, as described in Table 2.

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Specifying the authentication mode for user level switching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface [type] first-number [last-number]</td>
</tr>
<tr>
<td>Specify the authentication mode for user level switching</td>
<td>super authentication-mode</td>
</tr>
<tr>
<td></td>
<td>super-password</td>
</tr>
<tr>
<td>HWTACACS authentication</td>
<td>super authentication-mode scheme</td>
</tr>
<tr>
<td>Super password authentication preferred (with the HWTACACS authentication as the backup authentication mode)</td>
<td>super authentication-mode</td>
</tr>
<tr>
<td></td>
<td>super-password scheme</td>
</tr>
<tr>
<td>HWTACACS authentication preferred (with the super password authentication as the backup authentication mode)</td>
<td>super authentication-mode scheme</td>
</tr>
<tr>
<td></td>
<td>super-password</td>
</tr>
</tbody>
</table>

*When both the super password authentication and the HWTACACS authentication are specified, the device adopts the preferred authentication mode.*
first. If the preferred authentication mode cannot be implemented (for example, the super password is not configured or the HWTACACS authentication server is unreachable), the backup authentication mode is adopted.

Adopting super password authentication for user level switching

With the super password set, you can pass the super password authentication successfully only when you provide the super password when prompted. If no super password is set, the system prompts “%Password is not set” when you attempt to switch to a higher user level. In this case, you cannot pass the super password authentication.

Table 3 lists the operations to configure super password authentication for user level switching, which can only be performed by level-3 users.

Table 3  Setting a password for use level switching

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Set the super password for user level switching</td>
<td>super password [level] {cipher</td>
<td>simple} password</td>
</tr>
</tbody>
</table>

Adopting HWTACACS authentication for user level switching

To implement HWTACACS authentication for user level switching, a level-3 user must perform the commands listed in Table 4 to configure the HWTACACS authentication scheme used for low-to-high user level switching. With HWTACACS authentication enabled, you can pass the HWTACACS authentication successfully only after you provide the right user name and the corresponding password as prompted. Note that if you have passed the HWTACACS authentication when logging in to the switch, only the password is required.

Table 4 lists the operations to configure HWTACACS authentication for user level switching, which can only be performed by Level-3 users.

Table 4  Set the HWTACACS authentication scheme for user level switching

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter ISP domain view</td>
<td>domain domain-name</td>
<td>-</td>
</tr>
<tr>
<td>Set the HWTACACS authentication scheme for user level switching</td>
<td>authentication super hwtacacs-scheme hwtacacs-scheme-name</td>
<td>Required By default, the HWTACACS authentication scheme for user level switching is not set.</td>
</tr>
</tbody>
</table>

When setting the HWTACACS authentication scheme for user level switching using the authentication super hwtacacs-scheme command, make sure the HWTACACS authentication scheme identified by the hwtacacs-scheme-name argument already exists. Refer to the section entitled “Configuring TACACS Authentication Servers” on page 538 for details.
Switching to a specific user level

**Table 5  Switch to a specific user level**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Switch to a specified user level | `super [ level ]` | Required

Execute this command in user view.

- If no user level is specified in the `super password` command or the `super` command, level 3 is used by default.
- For security purposes, the password entered is not displayed when you switch to another user level. You will remain at the original user level if you have tried three times but failed to enter the correct authentication information.

**Configuration examples**

After a general user telnets to the switch, the user level is 0. The network administrator can allow general users to switch to level 3 so that they are able to configure the switch.

1. **Super password authentication configuration example:**

   # A level 3 user sets a switching password for user level 3.

   ```
   <5500> system-view
   [5500] super password level 3 simple 123
   ```

   # A general user telnets to the switch, and then uses the set password to switch to user level 3.

   ```
   <5500> super 3
   Password:
   User privilege level is 3, and only those commands can be used whose level is equal or less than this.
   Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
   ```

   # After configuring the switch, the general user switches back to user level 0.

   ```
   <5500> super 0
   User privilege level is 0, and only those commands can be used whose level is equal or less than this.
   Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
   ```

2. **HWTACACS authentication configuration example**

   # Configure an HWTACACS authentication scheme named acs, and specify the user name and password used for user level switching on the HWTACACS server defined in the scheme. Refer to the chapter entitled “AAA Configuration” page 519 for details.

   ```
   # Enable HWTACACS authentication for VTY 0 user level switching.
   <5500> system-view
   [5500] user-interface vty 0
   [5500-ui-vty0] super authentication-mode scheme
   [5500-ui-vty0] quit
   ```

   # Specify to adopt the HWTACACS authentication scheme named acs for user level switching in the ISP domain named system.

   ```
   [5500] domain system
   [5500-isp-system] authentication super hwtacacs-scheme acs
   ```
Command Hierarchy

Setting the Level of a Command in a Specific View

Commands fall into four levels:
- visit (level 0)
- monitor (level 1)
- system (level 2)
- manage (level 3).

By using the following command, the administrator can change the level of a command in a specific view as required.

**Table 6  Set the level of a command in a specific view**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the level of a command</td>
<td>command-privilege</td>
<td>Required</td>
</tr>
<tr>
<td>in a specific view</td>
<td>level view view</td>
<td>command</td>
</tr>
</tbody>
</table>

**CAUTION:**
- 3Com recommends that you do not to change the level of a command arbitrarily, for it may cause problems when operating and maintaining the switch.
- When you change the level of a command with multiple keywords, you should input the keywords one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect.

**Configuration example**
The network administrator (a level 3 user) changes TFTP commands (such as `tftp get`) from level 3 to level 0, so that general Telnet users (level 0 users) are able to download files through TFTP.

# Change the `tftp get` command in user view (shell) from level 3 to level 0. (By default, only level 3 users can change the level of a command.)

```
<5500> system-view
[5500] command-privilege level 0 view shell tftp
[5500] command-privilege level 0 view shell tftp 192.168.0.1
[5500] command-privilege level 0 view shell tftp 192.168.0.1 get
[5500] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm
```

This allows general Telnet users to use the `tftp get` command to download file `bootrom.btm` and other files from TFTP server 192.168.0.1 and other TFTP servers.
CLI Views

CLI views are designed for different configuration tasks. When you first log into the switch, you are in user view, where you can perform simple operations such as checking the operation status and statistics information of the switch. To enter the system view, execute the `system-view` command.

Table 7 lists the CLI views provided by the Switch 5500 Family, operations that can be performed in each view, and the commands used to enter each view.

<table>
<thead>
<tr>
<th>View</th>
<th>Available operation</th>
<th>Prompt example</th>
<th>Enter method</th>
<th>Quit method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User view</td>
<td>Display operation status and statistical information of the switch</td>
<td>&lt;5500&gt;</td>
<td>Enter user view once logging into the switch.</td>
<td>Execute the <code>quit</code> command to log out of the switch.</td>
</tr>
<tr>
<td>System view</td>
<td>Configure system parameters</td>
<td>[5500]</td>
<td>Execute the <code>system-view</code> command in user view.</td>
<td>Execute the <code>quit</code> or <code>return</code> command to return to user view.</td>
</tr>
<tr>
<td>Ethernet port view</td>
<td>Configure Ethernet port parameters</td>
<td>1000 Mbps Ethernet port view: [5500G-GigabitEthernet 1/0/1]</td>
<td>Execute the <code>interface gigabitethernet</code> command in system view.</td>
<td>Execute the <code>quit</code> command to return to system view. Execute the <code>return</code> command to return to user view.</td>
</tr>
<tr>
<td>Switch 5500G</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7 CLI views

<table>
<thead>
<tr>
<th>View</th>
<th>Available operation</th>
<th>Prompt example</th>
<th>Enter method</th>
<th>Quit method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet port view</td>
<td>Configure Ethernet port parameters</td>
<td>100 Mbps Ethernet port view: [5500-Ethernet1/0/1]</td>
<td>Execute the <strong>interface ethernet</strong> command in system view.</td>
<td>Execute the <strong>quit</strong> command to return to system view.</td>
</tr>
<tr>
<td>Switch 5500</td>
<td></td>
<td>1000 Mbps Ethernet port view: [5500-GigabitEthernet1/1/1]</td>
<td>Execute the <strong>interface gigabitethernet</strong> command in system view.</td>
<td>Execute the <strong>return</strong> command to return to user view.</td>
</tr>
<tr>
<td>VLAN view</td>
<td>Configure VLAN parameters</td>
<td>[5500-vlan1]</td>
<td>Execute the <strong>vlan</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>VLAN interface view</td>
<td>Configure VLAN interface parameters</td>
<td>[5500-Vlan-interface1]</td>
<td>Execute the <strong>interface Vlan-interface</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>Loopback interface view</td>
<td>Configure loopback interface parameters</td>
<td>[5500-LoopBack0]</td>
<td>Execute the <strong>interface loopback</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>NULL interface view</td>
<td>Configure NULL interface parameters</td>
<td>[5500-NUL0]</td>
<td>Execute the <strong>interface null</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>Cascade interface view</td>
<td>Configure Cascade interface parameters</td>
<td>[5500G-Cascade 1/2/1]</td>
<td>Execute the <strong>interface Cascade</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>(Switch 5500G only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local user view</td>
<td>Configure local user parameters</td>
<td>[5500-luser-user1]</td>
<td>Execute the <strong>local-user</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>User interface view</td>
<td>Configure user interface parameters</td>
<td>[5500-ui-aux0]</td>
<td>Execute the <strong>user-interface</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>FTP client view</td>
<td>Configure FTP client parameters</td>
<td>[ftp]</td>
<td>Execute the <strong>ftp</strong> command in user view.</td>
<td></td>
</tr>
<tr>
<td>SFTP client view</td>
<td>Configure SFTP client parameters</td>
<td>sftp-client&gt;</td>
<td>Execute the <strong>sftp</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>MST region view</td>
<td>Configure MST region parameters</td>
<td>[5500-mst-region]</td>
<td>Execute the <strong>stp region-configuration</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>Cluster view</td>
<td>Configure cluster parameters</td>
<td>[5500-cluster]</td>
<td>Execute the <strong>cluster</strong> command in system view.</td>
<td></td>
</tr>
<tr>
<td>Public key view</td>
<td>Configure the RSA public key for SSH users</td>
<td>[5500-rsa-public-key]</td>
<td>Execute the <strong>rsa peer-public-key</strong> command in system view.</td>
<td>Execute the <strong>peer-public-key end</strong> command to return to system view.</td>
</tr>
<tr>
<td></td>
<td>Configure the RSA or DSA public key for SSH users</td>
<td>[5500-peer-public-key]</td>
<td>Execute the <strong>public-key peer</strong> command in system view.</td>
<td></td>
</tr>
</tbody>
</table>
Public key editing view
Edit the RSA public key for SSH users
[5500-rsa-key-code]
Execute the public-key-code begin command in public key view.
Execute the public-key-code end command to return to public key view.

DHCP address pool view
Configure DHCP address pool parameters
[5500-dhcp-pool-a123]
Execute the dhcp server ip-pool command in system view.
Execute the quit command to return to system view.
Execute the return command to return to user view.

PIM view
Configure PIM parameters
[5500-pim]
Execute the pim command in system view.
If multicast routing is not enabled, you should first execute the multicast routing-enable command.
Execute the return command to return to user view.

RIP view
Configure RIP protocol parameters
[5500-rip]
Execute the rip command in system view.
Execute the quit command to return to system view.
Execute the return command to return to user view.

OSPF view
Configure OSPF protocol parameters
[5500-ospf-1]
Execute the ospf command in system view.
Execute the quit command to return to system view.
Execute the return command to return to user view.

OSPF area view
Configure OSPF area parameters
[5500-ospf-1-area-0.0.0.1]
Execute the area command in OSPF view.
Execute the quit command to return to OSPF view.
Execute the return command to return to user view.

BGP view
Switch 5500G only
Configure BGP protocol parameters
[5500G-bgp]
Execute the bgp command in system view.
Execute the quit command to return to system view.
Execute the return command to return to user view.

BGP IPv4 multicast address family view
Switch 5500G only
Configure the BGP IPv4 multicast address family
[5500G-bgp-af-mul]
Execute the ipv4-family multicast command in OSPF view
Execute the quit command to return to system view.
Execute the return command to return to user view.

Routing policy view
Configure routing policy
[5500-route-policy]
Execute the route-policy command in system view.
Execute the quit command to return to system view.
Execute the return command to return to user view.

Basic ACL view
Define rules for a basic ACL (with ID ranging from 2000 to 2999)
[5500-acl-basic-2000]
Execute the acl number command in system view.

Advanced ACL view
Define rules for an advanced ACL (with ID ranging from 3000 to 3999)
[5500-acl-adv-3000]
Execute the acl number command in system view.

Layer 2 ACL view
Define rules for a Layer 2 ACL (with ID ranging from 4000 to 4999)
[5500-acl-ethernetframe-4000]
Execute the acl number command in system view.

User-defined ACL view
Define rules for a user-defined ACL (with ID ranging from 5000 to 5999)
[5500-acl-user-5000]
Execute the acl number command in system view.
The shortcut key <Ctrl+Z> is equivalent to the return command.

**CLI Features**

**Online Help**  When configuring the switch, you can use the online help to get related help information. The CLI provides two types of online help: complete and partial.
CHAPTER 1: CLI CONFIGURATION

Complete online help

1. Enter a question mark (?) in any view to display all the commands available in the view and a brief description for each command, for example:

   `<5500>` ?

   User view commands:
   - `backup`  Backup current configuration
   - `boot`    Set boot option
   - `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` Display current system information

2. Enter a command, a space, and a question mark (?).

   If the question mark “?” is at a keyword position in the command, all available keywords at the position and their descriptions will be displayed on your terminal.

   `<5500>` clock ?

   User view commands:
   - `datetime` Specify the time and date
   - `summer-time` Configure summer time
   - `timezone`  Configure time zone

   If the question mark “?” is at an argument position in the command, the description of the argument displays:

   `[5500]` interface vlan-interface ?
   - `<1-4094>` VLAN interface number

   If only <cr> is displayed after you enter “?”, it means no parameter is available at the “?” position, and you can enter and execute the command directly.

   `[5500]` interface vlan-interface 1 ?
   <cr>

Partial online help

1. Enter a character/string, and followed by a question mark (?). All the commands beginning with the character/string display, for example:

   `<5500>` p?
   - ping
   - pwd

2. Enter a command, a space, and a character/string followed by a question mark (?). All the keywords beginning with the character/string (if available) display, for example:

   `<5500>` display v?
   - version
   - vlan
   - voice
   - vrrp

3. Enter the first several characters of a command’s keyword and then press <Tab>. If there is a unique keyword beginning with the characters just typed, the unique keyword is displayed in its complete form. If there are multiple keywords
beginning with the characters, you can display them one by one (in complete form) by pressing <Tab> repeatedly.

**Terminal Display**

The CLI provides the screen splitting feature display output suspended when the screen is full. When display output pauses, you can perform the following operations as needed.

**Table 8** Display-related operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press &lt;Ctrl+C&gt;</td>
<td>Stop the display output and execution of the command.</td>
</tr>
<tr>
<td>Press any character except &lt;Space&gt;, &lt;Enter&gt;, /, +, and - when the display output pauses</td>
<td>Stop the display output.</td>
</tr>
<tr>
<td>Press the space key</td>
<td>Get to the next page.</td>
</tr>
<tr>
<td>Press &lt;Enter&gt;</td>
<td>Get to the next line.</td>
</tr>
</tbody>
</table>

**Command History**

The CLI provides the command history function. You can use the `display history-command` command to view a specific number of latest executed commands and execute them again. By default, the CLI stores up to 10 most recently executed commands for each user. You can view the command history by performing the operations listed in Table 9.

**Table 9** View history commands

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Operation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the latest executed history commands</td>
<td>Execute the <code>display history-command</code> command</td>
<td>This command displays the command history.</td>
</tr>
<tr>
<td>Recall the previous history command</td>
<td>Press the up arrow key or &lt;Ctrl+P&gt;</td>
<td>This operation recalls the previous history command (if available).</td>
</tr>
<tr>
<td>Recall the next history command</td>
<td>Pressing the down arrow key or &lt;Ctrl+N&gt;</td>
<td>This operation recalls the next history command (if available).</td>
</tr>
</tbody>
</table>

- The Windows 9x HyperTerminal defines the up and down arrow keys in a different way, and therefore the two keys are invalid when you access history commands in such an environment. However, you can use <Ctrl+P> and <Ctrl+N> instead to achieve the same purpose.

- When you enter the same command multiple times consecutively, only one history command entry is stored in the CLI.

**Error Prompts**

If a command passes the syntax check, it is executed; otherwise, an error message displays. Table 10 lists the most common error messages.

**Table 10** Common error messages

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrecognized command</td>
<td>The command does not exist. The keyword does not exist. The parameter type is wrong. The parameter value is out of range.</td>
</tr>
</tbody>
</table>
CHAPTER 1: CLI CONFIGURATION

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 11 lists the CLI edit operations.

### Table 10  Common error messages

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete command</td>
<td>The command entered is incomplete.</td>
</tr>
<tr>
<td>Too many parameters</td>
<td>You entered too many parameters.</td>
</tr>
<tr>
<td>Ambiguous command</td>
<td>The parameters entered are ambiguous.</td>
</tr>
<tr>
<td>Wrong parameter</td>
<td>A parameter entered is wrong.</td>
</tr>
<tr>
<td>found at <code>^</code> position</td>
<td>An error is found at the <code>^</code> position.</td>
</tr>
</tbody>
</table>

### Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 11 lists the CLI edit operations.

### Table 11  Edit operations

<table>
<thead>
<tr>
<th>Press...</th>
<th>To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A common key</td>
<td>Insert the corresponding character at the cursor position and move the cursor one character to the right if the command is shorter than 254 characters.</td>
</tr>
<tr>
<td>Backspace key</td>
<td>Delete the character on the left of the cursor and move the cursor one character to the left.</td>
</tr>
<tr>
<td>Left arrow key or &lt;Ctrl+B&gt;</td>
<td>Move the cursor one character to the left.</td>
</tr>
<tr>
<td>Right arrow key or &lt;Ctrl+F&gt;</td>
<td>Move the cursor one character to the right.</td>
</tr>
<tr>
<td>Up arrow key or &lt;Ctrl+P&gt;</td>
<td>Display history commands.</td>
</tr>
<tr>
<td>Down arrow key or &lt;Ctrl+N&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;Tab&gt;</td>
<td>Use the partial online help. That is, when you input an incomplete keyword and press &lt;Tab&gt;, if the input parameter uniquely identifies a complete keyword, the system substitutes the complete keyword for the input parameter; if more than one keywords match the input parameter, you can display them one by one (in complete form) by pressing &lt;Tab&gt; repeatedly; if no keyword matches the input parameter, the system displays your original input on a new line without any change.</td>
</tr>
</tbody>
</table>
LOGGING INTO AN ETHERNET SWITCH

Logging into an Ethernet Switch

You can log into a Switch 5500 in one of the following ways:

- Logging in locally through the console port
- Logging in locally or remotely through an Ethernet port by means of Telnet or SSH
- Using Telnet to access the console port using a modem
- Logging into the Web-based network management system
- Logging in through NMS (network management station)

Introduction to the User Interface

Supported User Interfaces

The Switch 5500’s auxiliary (AUX) port and the console port are the same port (referred to as console port in the following section). When logging into this port, you are in the AUX user interface.

The Switch 5500 Family support two types of user interfaces, AUX and VTY.

- **AUX user interface**: A view when you log in through the AUX port. AUX port is a line device port.
- **Virtual type terminal (VTY) user interface**: A view when you log in through VTY. VTY port is a logical terminal line used when you access the device by means of Telnet or SSH.

<table>
<thead>
<tr>
<th>User interface</th>
<th>Applicable user</th>
<th>Port used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUX</td>
<td>Users logging in through the console port</td>
<td>Console port</td>
<td>Each switch can accommodate one AUX user.</td>
</tr>
<tr>
<td>VTY</td>
<td>Telnet users and SSH users</td>
<td>Ethernet port</td>
<td>Each switch can accommodate up to five VTY users.</td>
</tr>
</tbody>
</table>
User Interface Index

There are two types of user interface indexes, absolute user interface index and relative user interface index.

1. The absolute user interface indexes are as follows:
   - The absolute AUX user interfaces are numbered 0 through 7.
   - VTY user interface indexes follow AUX user interface indexes. The first absolute VTY user interface is numbered 8, the second is 9, and so on.

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 interfaces are numbered from AUX0 to AUX7.
   - VTY user interfaces are numbered VTY0, VTY1, and so on.

The Switch 5500 Family supports Fabric. A Fabric can contain up to eight devices. Accordingly, the AUX user interfaces in a Fabric can be numbered from AUX0 to AUX7, through which all the console ports of the units in a Fabric can be identified. Refer to the chapter entitled “IRF Fabric Configuration” on page 733 for more information about Fabrics.

Common User Interface Configuration

Table 13 Common user interface configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock the current user</td>
<td>lock</td>
<td>Optional&lt;br&gt;Execute this command in user view.&lt;br&gt;A user interface is not locked by default.</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify to send messages</td>
<td>send { all</td>
<td>number</td>
</tr>
<tr>
<td>to all user interfaces/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specified user interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free a user interface</td>
<td>free user-interface { type }</td>
<td>Optional&lt;br&gt;Execute this command in user view.</td>
</tr>
<tr>
<td></td>
<td>number</td>
<td></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set the banner</td>
<td>header</td>
<td>incoming</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set a system name for the</td>
<td>sysname string</td>
<td>Optional&lt;br&gt;By default, the system name is 5500.</td>
</tr>
<tr>
<td>switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable copyright</td>
<td>copyright-info enable</td>
<td>Optional&lt;br&gt;By default, copyright displaying is enabled. That is, the copy right information is displayed on the terminal after a user logs in successfully.</td>
</tr>
<tr>
<td>information displaying</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface { type }</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>first-number</td>
<td>last-number</td>
</tr>
</tbody>
</table>
Table 13  Common user interface configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about the current user</td>
<td><code>display users [ all ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>interface/all user interfaces</td>
<td></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display the physical attributes and configuration</td>
<td>`display user-interface [</td>
<td></td>
</tr>
<tr>
<td>of the current/a specified</td>
<td>type number</td>
<td>number ]</td>
</tr>
<tr>
<td>user interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display the information about the current web users</td>
<td><code>display web users</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**LOGGING IN THROUGH THE CONSOLE PORT**

**Introduction**

To log in through the console port is the most common way to log into a switch. It is also the prerequisite to configure other login methods. By default, you can locally log into a Switch 5500 through its console port only.

Table 14 lists the default settings of a console port.

**Table 14** The default settings of a console port

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud rate</td>
<td>9,600 bps</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
<tr>
<td>Check mode (Parity)</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
</tbody>
</table>

To log into a switch through the console port, make sure the settings of both the console port and the user terminal are the same.

After logging into a switch, you can perform configuration for AUX users. Refer to “Console Port Login Configuration” on page 38.

**Logging In Through the Console Port**

The following procedure describes how to connect to a switch through the console port.

1. Connect the serial port of your PC/terminal to the console port of the switch, as shown in Figure 1.

   ![Figure 1](image.png)

2. 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. The following assumes that you are running Windows XP) and perform the configuration shown in Figure 2 through Figure 4 for the connection to be created. Normally, both sides (that is, the serial port of the PC and the console port of the switch) are configured as those listed in Table 14.
**Figure 2** Create a connection

![Connection Description](image)

**Figure 3** Specify the port used to establish the connection

![Connect To](image)
3 Turn on the switch. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as <5500>) appears after you press the Enter key, as shown in Figure 5.

4 You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character.
CHAPTER 3: LOGGING IN THROUGH THE CONSOLE PORT

Console Port Login
Configuration

Common Configuration

Table 15 lists the common configuration of console port login.

Table 15  Common console port login configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud rate</td>
<td>Optional</td>
</tr>
<tr>
<td>The default baud rate is 9,600 bps.</td>
<td></td>
</tr>
<tr>
<td>Check mode</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the check mode of the console port is set to “none”, which means no check bit.</td>
<td></td>
</tr>
<tr>
<td>Stop bits</td>
<td>Optional</td>
</tr>
<tr>
<td>The default stop bits of a console port is 1.</td>
<td></td>
</tr>
<tr>
<td>Data bits</td>
<td>Optional</td>
</tr>
<tr>
<td>The default data bits of a console port is 8.</td>
<td></td>
</tr>
<tr>
<td>Configure the command level available to the users logging into the AUX user interface</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, commands of level 3 are available to the users logging into the AUX user interface.</td>
<td></td>
</tr>
<tr>
<td>Make terminal services available</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, terminal services are available in all user interfaces</td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of lines the screen can contain</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the screen can contain up to 24 lines.</td>
<td></td>
</tr>
<tr>
<td>Set history command buffer size</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the history command buffer can contain up to 10 commands.</td>
<td></td>
</tr>
<tr>
<td>Set the timeout time of a user interface</td>
<td>Optional</td>
</tr>
<tr>
<td>The default timeout time is 10 minutes.</td>
<td></td>
</tr>
</tbody>
</table>

CAUTION: The change to console port configuration takes effect immediately, so the connection may be disconnected when you log in through a console port and then configure this console port. To configure a console port, you are recommended to log into the switch in other ways. To log into a switch through its console port after you modify the console port settings, you need to modify the corresponding settings of the terminal emulation utility running on your PC accordingly in the dialog box shown in Figure 4.
Table 16 lists console port login configurations for different authentication modes.

### Table 16  Console port login configurations for different authentication modes

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Console port login configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Perform common configuration</td>
<td>Optional Refer to Table 15.</td>
</tr>
<tr>
<td>Password</td>
<td>Configure the password</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Perform common configuration</td>
<td>Optional Refer to Table 15.</td>
</tr>
<tr>
<td>Scheme</td>
<td>Specify to perform local authentication or remote RADIUS authentication</td>
<td>Optional Local authentication is performed by default. Refer to “AAA Configuration” on page 519.</td>
</tr>
<tr>
<td></td>
<td>Configure user names and passwords for local/RADIUS users</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>- The user name and password of a local user are configured on the switch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The user name and password of a RADIUS user are configured on the RADIUS server. Refer to the RADIUS server’s user manual for more information.</td>
<td></td>
</tr>
<tr>
<td>Manage AUX users</td>
<td>Set service type for AUX users</td>
<td>Required</td>
</tr>
<tr>
<td>Perform common configuration</td>
<td>Perform common configuration for console port login</td>
<td>Optional Refer to Table 15.</td>
</tr>
</tbody>
</table>

Changes made to the authentication mode for console port login takes effect after you quit the command-line interface and then log in again.

### Configuration Procedure

Perform the steps in Table 17 to configure console port login with authentication mode being none.

### Table 17  Console port login configuration with the authentication mode being none

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter AUX user interface view</td>
<td>user-interface aux 0</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 17  Console port login configuration with the authentication mode being none

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure not to authenticate users</td>
<td>authentication-mode none</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, users logging in through the console port (AUX user interface) are not authenticated.</td>
</tr>
<tr>
<td>Configure the console port</td>
<td>Set the baud rate</td>
<td>speed speed-value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default baud rate of a console port is 9,600 bps.</td>
</tr>
<tr>
<td></td>
<td>Set the check mode</td>
<td>parity { even</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the check mode of a console port is none, that is, no check is performed.</td>
</tr>
<tr>
<td></td>
<td>Set the stop bits</td>
<td>stopbits { 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The stop bits of a console port is 1.</td>
</tr>
<tr>
<td></td>
<td>Set the data bits</td>
<td>databits { 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default data bits of a console port is 8.</td>
</tr>
<tr>
<td>Configure the command level available to users</td>
<td>user privilege level level</td>
<td>Optional</td>
</tr>
<tr>
<td>logging into the user interface</td>
<td></td>
<td>By default, commands of level 3 are available to users logging into the AUX user interface, and commands of level 0 are available to users logging into the VTY user interface.</td>
</tr>
<tr>
<td>Enable terminal services</td>
<td>shell</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, terminal services are available in all user interfaces.</td>
</tr>
<tr>
<td>Set the maximum number of lines the screen can</td>
<td>screen-length screen-length</td>
<td>Optional</td>
</tr>
<tr>
<td>contain</td>
<td></td>
<td>By default, the screen can contain up to 24 lines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the screen-length 0 command to disable the function to display information in pages.</td>
</tr>
<tr>
<td>Set the history command buffer size</td>
<td>history-command max-size value</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.</td>
</tr>
</tbody>
</table>
Table 17  Console port login configuration with the authentication mode being none

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set the timeout time for the user interface | idle-timeout minutes [ seconds ] | Optional
The default timeout time of a user interface is 10 minutes.
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.
You can use the idle-timeout 0 command to disable the timeout function. |

Configuration Example

Network requirements

Assume that the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Do not authenticate the users.
- Commands of level 2 are available to the users logging into 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 contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.
CHAPTER 3: LOGGING IN THROUGH THE CONSOLE PORT

Network diagram

Figure 6  Network diagram for AUX user interface configuration (with the authentication mode being none)

Configuration procedure

# Enter system view.

<5500> system-view

# Enter AUX user interface view.

[5500] user-interface aux 0

# Specify not to authenticate users logging in through the console port.

[5500-ui-aux0] authentication-mode none

# Specify commands of level 2 are available to users logging into the AUX user interface.

[5500-ui-aux0] user privilege level 2

# Set the baud rate of the console port to 19,200 bps.

[5500-ui-aux0] speed 19200

# Set the maximum number of lines the screen can contain to 30.

[5500-ui-aux0] screen-length 30

# Set the maximum number of commands the history command buffer can store to 20.

[5500-ui-aux0] history-command max-size 20

# Set the timeout time of the AUX user interface to 6 minutes.
After completing the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 4 to log into the switch successfully.

### Console Port Login Configuration with Authentication Mode Being Password

Perform the steps in Table 18 to configure console port login with authentication mode being password.

#### Configuration Procedure

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter AUX user interface view</td>
<td>user-interface aux 0</td>
<td>-</td>
</tr>
<tr>
<td>Configure to authenticate users using the local password</td>
<td>authentication-mode password</td>
<td>Required By default, users logging into a switch through the console port are not authenticated; while those logging in through Modems or Telnet are authenticated.</td>
</tr>
<tr>
<td>Set the local password</td>
<td>set authentication password { cipher</td>
<td>simple } password</td>
</tr>
<tr>
<td>Configure the console port</td>
<td>speed speed-value</td>
<td>Optional The default baud rate of an AUX port (also the console port) is 9,600 bps.</td>
</tr>
<tr>
<td>Set the check mode</td>
<td>parity { even</td>
<td>none</td>
</tr>
<tr>
<td>Set the stop bits</td>
<td>stopbits { 1</td>
<td>1.5</td>
</tr>
<tr>
<td>Set the data bits</td>
<td>databits { 7</td>
<td>8 }</td>
</tr>
<tr>
<td>Configure the command level available to users logging into the user interface</td>
<td>user privilege level level</td>
<td>Optional By default, commands of level 3 are available to users logging into the AUX user interface.</td>
</tr>
<tr>
<td>Make terminal services available to the user interface</td>
<td>shell</td>
<td>Optional By default, terminal services are available in all user interfaces.</td>
</tr>
</tbody>
</table>
### Configuration Example

#### Network requirements

Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Authenticate the users using passwords.
- Set the local password to 123456 (in plain text).
- The commands of level 2 are available to the users.
- 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.

---

**Table 18** Console port login configuration with the authentication mode being password

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the maximum number of lines</td>
<td><code>screen-length</code></td>
<td>Optional</td>
</tr>
<tr>
<td>of lines the screen can contain</td>
<td><code>screen-length</code></td>
<td>By default, the screen can contain up to 24 lines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the <code>screen-length 0</code> command to disable the function to display information in pages.</td>
</tr>
<tr>
<td>Set history command buffer size</td>
<td><code>history-command</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><code>max-size value</code></td>
<td>The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.</td>
</tr>
<tr>
<td>Set the timeout time for the</td>
<td><code>idle-timeout</code></td>
<td>Optional</td>
</tr>
<tr>
<td>user interface</td>
<td><code>minutes [seconds ]</code></td>
<td>The default timeout time of a user interface is 10 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the <code>idle-timeout 0</code> command to disable the timeout function.</td>
</tr>
</tbody>
</table>
Network diagram

Figure 7  Network diagram for AUX user interface configuration (with the authentication mode being password)

Configuration procedure

# Enter system view.

<5500> system-view

# Enter AUX user interface view.

[5500] user-interface aux 0

# Specify to authenticate users logging in through the console port using the local password.

[5500-ui-aux0] authentication-mode password

# Set the local password to 123456 (in plain text).

[5500-ui-aux0] set authentication password simple 123456

# Specify commands of level 2 are available to users logging into the AUX user interface.

[5500-ui-aux0] user privilege level 2

# Set the baud rate of the console port to 19,200 bps.

[5500-ui-aux0] speed 19200

# Set the maximum number of lines the screen can contain to 30.

[5500-ui-aux0] screen-length 30

# Set the maximum number of commands the history command buffer can store to 20.

[5500-ui-aux0] history-command max-size 20
# Set the timeout time of the AUX user interface to 6 minutes.

```
[5500-ui-aux0] idle-timeout 6
```

After completing the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 4 to log into the switch successfully.

## Console Port Login Configuration with Authentication Mode Being Scheme

Perform the steps in Table 19 to configure console port login with authentication mode being scheme.

### Configuration Procedure

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
</tbody>
</table>
| Configure the authentication mode | `domain domain-name` | Optional 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. If you specify to apply an existing scheme by providing the `radius-scheme-name` argument, you need to perform the following configuration as well:  
- Perform AAA&RADIUS configuration on the switch. (Refer to "AAA Configuration" on page 519 for more information.)  
- Configure the user name and password accordingly on the AAA server. (Refer to the AAA server’s user manual.) |
| Specify the AAA scheme to be applied to the domain | `scheme { local | none | radius-scheme radius-scheme-name [ local ] | hwtacacs-scheme hwtacacs-scheme-name [ local ] }` | |
| Quit to system view | `quit` | |
| Create a local user (Enter local user view.) | `local-user user-name` | Required |
| Set the authentication password for the local user | `password { simple | cipher } password` | Required |
| Specify the service type for AUX users | `service-type terminal [ level level ]` | Required |
| Quit to system view | `quit` | - |
| Enter AUX user interface view | `user-interface aux 0` | - |
## Table 19  Console port login configuration with the authentication mode being scheme

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure to authenticate users locally or remotely                       | authentication-mode scheme { command-authorization } | Required  
The specified AAA scheme determines whether to authenticate users locally or remotely.  
By default, users logging in through the console port (AUX user interface) are not authenticated. |
| Configure the console port                                               | speed speed-value                          | Optional  
The default baud rate of the AUX port (also the console port) is 9,600 bps. |
| Set the check mode                                                        | parity { even | none | odd }                                   | Optional  
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  
The default stop bits of a console port is 1. |
| Set the data bits                                                         | databits { 7 | 8 }                              | Optional  
The default data bits of a console port is 8. |
| Configure the command level available to users logging into the user interface | user privilege level level | Optional  
By default, commands of level 3 are available to users logging into the AUX user interface. |
| Make terminal services available to the user interface                    | shell                                       | Optional  
By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain                    | screen-length                              | Optional  
By default, the screen can contain up to 24 lines.  
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  
The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default. |
CHAPTER 3: LOGGING IN THROUGH THE CONSOLE PORT

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging into a switch depends on the command level specified in the `service-type terminal [ level level ]` command.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set the timeout time for the user interface | `idle-timeout minutes [ seconds ]` | Optional
| | | The default timeout time of a user interface is 10 minutes.
| | | 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.
| | | You can use the `idle-timeout 0` command to disable the timeout function. |

Table 19: Console port login configuration with the authentication mode being scheme

Configuration Example

Network requirements
Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Configure the local user name as `guest`.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of the local user to Terminal and the command level to 2.
- Configure to authenticate the users 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.
Configuration procedure

# Enter system view.

<5500> system-view

# Create a local user named guest and enter local user view.

[5500] local-user guest

# Set the authentication password to 123456 (in plain text).

[5500-luser-guest] password simple 123456

# Set the service type to Terminal, Specify commands of level 2 are available to users logging into the AUX user interface.

[5500-luser-guest] service-type terminal level 2
[5500-luser-guest] quit

# Enter AUX user interface view.

[5500] user-interface aux 0

# Configure to authenticate users logging in through the console port in the scheme mode.

[5500-ui-aux0] authentication-mode scheme

# Set the baud rate of the console port to 19,200 bps.

[5500-ui-aux0] speed 19200

# Set the maximum number of lines the screen can contain to 30.

[5500-ui-aux0] screen-length 30
# Set the maximum number of commands the history command buffer can store to 20.

[5500-ui-aux0] history-command max-size 20

# Set the timeout time of the AUX user interface to 6 minutes.

[5500-ui-aux0] idle-timeout 6

After completing the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 4 to log into the switch successfully.
LOGGING IN THROUGH TELNET

Introduction

The Switch 5500 Family supports Telnet. You can manage and maintain a switch remotely by using Telnet to access the switch. To log into a switch through Telnet, the corresponding configuration is required on both the switch and the Telnet terminal.

You can also log into a switch through SSH. SSH is a secure shell added to Telnet. Refer to “SSH Configuration” on page 833 for related information.

Table 20 Requirements for using Telnet to access a switch

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>The IP address is configured for the VLAN of the switch, and the route between the switch and the Telnet terminal is reachable. (Refer to “IP Addressing Configuration” on page 123, “IP Performance Configuration” on page 129, and “IP Routing Protocol Overview” on page 277.) The authentication mode and other settings are configured. Refer to Table 21 and Table 22.</td>
</tr>
<tr>
<td>Telnet terminal</td>
<td>Telnet is running. The IP address of the VLAN of the switch is available.</td>
</tr>
</tbody>
</table>

Telnetting to a switch using IPv6 protocols is similar to Telnetting to a switch using IPv4 protocols. Refer to “IPv6 Configuration” on page 995 for related information.

Common Configuration

Table 21 lists the common Telnet configuration.

Table 21 Common Telnet configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTY user interface configuration</td>
<td>Configure the command level available to users logging into the VTY user interface. By default, commands of level 0 are available to users logging into a VTY user interface.</td>
</tr>
<tr>
<td></td>
<td>Configure the protocols the user interface supports. By default, Telnet and SSH protocol are supported.</td>
</tr>
<tr>
<td></td>
<td>Set the commands to be executed automatically after a user log into the user interface successfully. By default, no command is executed automatically after a user logs into the VTY user interface.</td>
</tr>
</tbody>
</table>
### Table 21 Common Telnet Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTY terminal configuration</td>
<td>Optional By default, terminal services are available in all user interfaces.</td>
</tr>
<tr>
<td>Set the maximum number of lines the screen can contain</td>
<td>Optional By default, the screen can contain up to 24 lines.</td>
</tr>
<tr>
<td>Set history command buffer size</td>
<td>Optional By default, the history command buffer can contain up to 10 commands.</td>
</tr>
<tr>
<td>Set the timeout time of a user interface</td>
<td>Optional The default timeout time is 10 minutes.</td>
</tr>
</tbody>
</table>

### Telnet Configurations for Different Authentication Modes

Table 22 lists Telnet configurations for different authentication modes.

### Table 22 Telnet configurations for different authentication modes

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Telnet configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Perform common configuration</td>
<td>Optional Refer to Table 21.</td>
</tr>
<tr>
<td>Password</td>
<td>Configure the password</td>
<td>Required</td>
</tr>
<tr>
<td>Scheme</td>
<td>Specify to perform local authentication or remote RADIUS authentication</td>
<td>Optional Local authentication is performed by default. Refer to “AAA Configuration” on page 519.</td>
</tr>
<tr>
<td></td>
<td>Configure user name and password</td>
<td>Required ■ The user name and password of a local user are configured on the switch. ■ The user name and password of a remote user are configured on the RADIUS server. Refer to the RADIUS server’s user manual.</td>
</tr>
<tr>
<td></td>
<td>Manage VTY users</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Perform common configuration</td>
<td>Optional Refer to Table 21.</td>
</tr>
</tbody>
</table>
To improve security and prevent attacks to the unused Sockets, TCP 23 and TCP 22, ports for Telnet and SSH services respectively, will be enabled or disabled after corresponding configurations.

- If the authentication mode is `none`, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is `password`, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is `scheme`, there are three scenarios: when the supported protocol is specified as `telnet`, TCP 23 will be enabled; when the supported protocol is specified as `ssh`, TCP 22 will be enabled; when the supported protocol is specified as `all`, both the TCP 23 and TCP 22 port will be enabled.

### Telnet Configuration with Authentication Mode Being None

Perform the steps in Table 23 to configure Telnet with authentication mode being none.

#### Configuration Procedure

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter one or more VTY user interface views</td>
<td><code>user-interface vty first-number [last-number]</code></td>
<td>-</td>
</tr>
</tbody>
</table>
| Configure not to authenticate users logging into VTY user interfaces | `authentication-mode none` | Required
| | | By default, VTY users are authenticated after logging in. |
| Configure the command level available to users logging into VTY user interface | `user privilege level level` | Optional
| | | By default, commands of level 0 are available to users logging into VTY user interfaces. |
| Configure the protocols to be supported by the VTY user interface | `protocol inbound { all | ssh | telnet }` | Optional
| | | By default, both Telnet protocol and SSH protocol are supported. |
| Set the commands to be executed automatically after a user login to the user interface successfully | `auto-execute command text` | Optional
| | | By default, no command is executed automatically after a user logs into the VTY user interface. |
| Make terminal services available | `shell` | Optional
| | | 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
| | | By default, the screen can contain up to 24 lines. |

You can use the `screen-length 0` command to disable the function to display information in pages.
CHAPTER 4: LOGGING IN THROUGH TELNET

Note that if you configure not to authenticate the users, the command level available to users logging into a switch depends on the `user privilege level level` command.

**Configuration Example**

**Network requirements**

Assume that the current user logs in through the console port and that the user level is set to the administrator level (level 3). Perform the following configuration for users logging in through VTY 0 using Telnet.

- Do not authenticate the users.
- Level 2 commands are available to the users.
- 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 9*  Network diagram for Telnet configuration (with the authentication mode being none)

**Configuration procedure**

# Enter system view.

<5500> system-view

**Table 23**  Telnet configuration with the authentication mode being none

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set the history command buffer size | `history-command max-size value` | Optional
| | | 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
| | | The default timeout time of a user interface is 10 minutes. 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. You can use the `idle-timeout 0` command to disable the timeout function. |
Configuring Telnet with the Password Authentication Mode

Perform the steps in Table 24 to configure Telnet with “password” as the authentication mode.

### Configuration Procedure

**Table 24** Configuring Telnet with the password as the authentication mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter one or more VTY user interface views</td>
<td>user-interface vty first-number [ last-number ]</td>
<td></td>
</tr>
<tr>
<td>Configure to authenticate users logging into VTY user interfaces using the local password</td>
<td>authentication-mode password</td>
<td>Required</td>
</tr>
<tr>
<td>Set the local password</td>
<td>set authentication password ( cipher</td>
<td>simple ) password</td>
</tr>
<tr>
<td>Configure the command level available to users logging into the user interface</td>
<td>user privilege level level</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the protocol to be supported by the user interface</td>
<td>protocol inbound ( all</td>
<td>ssh</td>
</tr>
</tbody>
</table>

By default, commands of level 0 are available to users logging into VTY user interface.

By default, both Telnet protocol and SSH protocol are supported.
When the authentication mode is password, the command level available to users logging into the user interface is determined by the user privilege level command.

### Configuration Example

**Network requirements**

The current user logs in through the console port and the user level is set to the administrator level (level 3). Perform the following configuration for users logging into VTY 0 using Telnet.

1. Authenticate users using the local password.
2. Set the local password to 123456 (in plain text).
- Commands of level 2 are available to the users.
- 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 10* Network diagram for Telnet configuration (with the authentication mode being password)

![Network diagram for Telnet configuration](image)

**Configuration procedure**

```bash
# Enter system view.
<5500> system-view

# Enter VTY 0 user interface view.
[5500] user-interface vty 0

# Configure to authenticate users logging into VTY 0 using the password.
[5500-ui-vty0] authentication-mode password

# Set the local password to 123456 (in plain text).
[5500-ui-vty0] set authentication password simple 123456

# Specify commands of level 2 are available to users logging into VTY 0.
[5500-ui-vty0] user privilege level 2

# Configure Telnet protocol is supported.
[5500-ui-vty0] protocol inbound telnet

# Set the maximum number of lines the screen can contain to 30.
[5500-ui-vty0] screen-length 30

# Set the maximum number of commands the history command buffer can store to 20.
[5500-ui-vty0] history-command max-size 20

# Set the timeout time to 6 minutes.
[5500-ui-vty0] idle-timeout 6
```
Telnet Configuration with Authentication Mode Being Scheme

Perform the steps in Table 25 to configure Telnet with authentication mode being scheme.

**Configuration Procedure**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the authentication scheme</td>
<td>domain domain-name</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the AAA scheme to be applied to the domain</td>
<td>scheme ( \text{local</td>
<td>none</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Create a local user and enter local user view</td>
<td>local-user user-name</td>
<td>No local user exists by default.</td>
</tr>
<tr>
<td>Set the authentication password for the local user</td>
<td>password ( \text{simple</td>
<td>cipher } ) password</td>
</tr>
<tr>
<td>Specify the service type for VTY users</td>
<td>service-type telnet ( \text{level level} )</td>
<td>Required</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter one or more VTY user interface views</td>
<td>user-interface vty ( \text{first-number [ last-number]} )</td>
<td>Required</td>
</tr>
<tr>
<td>Configure to authenticate users locally or remotely</td>
<td>authentication-mode scheme ( \text{command-authorization} )</td>
<td>The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.</td>
</tr>
<tr>
<td>Configure the command level available to users logging into the user interface</td>
<td>user privilege level level</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the supported protocol</td>
<td>protocol inbound ( \text{all</td>
<td>ssh</td>
</tr>
<tr>
<td>Make terminal services available</td>
<td>shell</td>
<td>Optional</td>
</tr>
</tbody>
</table>

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.

- Perform AAA&RADIUS configuration on the switch. (Refer to “AAA Configuration” on page 519.)
- Configure the user name and password accordingly on the AAA server. (Refer to “AAA Configuration” on page 519.)
If you configure to authenticate the users in the scheme mode, the command level available to the users logging into the switch depends on the `user privilege level` command and the `service-type { ftp | lan-access | { ssh | telnet | terminal }* [ level level ] }` command, as listed in Table 26.
Refer to “AAA Configuration” on page 519 and “SSH Configuration” on page 833 for information about AAA, RADIUS, and SSH.
Configuration Example

Network requirements
Assume current user logins through the console port and the user level is set to the administrator level (level 3). Perform the following configurations for users logging into VTY 0 using Telnet.

- Configure the local user name as guest.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of VTY users to Telnet and the command level to 2.
- Configure to authenticate users logging into VTY 0 in scheme mode.
- Only 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 11 Network diagram for Telnet configuration (with the authentication mode being scheme)

Configuration procedure

# Enter system view.
<5500> system-view

# Create a local user named guest and enter local user view.
[5500] local-user guest

# Set the authentication password of the local user to 123456 (in plain text).
[5500-luser-guest] password simple 123456

# Set the service type to Telnet, Specify commands of level 2 are available to users logging into VTY 0..
[5500-luser-guest] service-type telnet level 2
[5500-luser-guest] quit

# Enter VTY 0 user interface view.
[5500] user-interface vty 0

# Configure to authenticate users logging into VTY 0 in the scheme mode.
[5500-ui-vty0] authentication-mode scheme

# Configure Telnet protocol is supported.
CHAPTER 4: LOGGING IN THROUGH TELNET

Using Telnet to Connect to a Switch

Using Telnet to Connect from a Terminal to a Switch

1 Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch).
   ■ Connect the serial port of your PC/terminal to the console port of the switch, as shown in Figure 12.

Figure 12 Diagram for establishing connection to a console port

- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt (such as <5500>) appears, as shown in the following figure.
Perform the following operations in the terminal window to assign IP address 202.38.160.92/24 to VLAN-interface 1 of the switch.

```
<5500> system-view
[5500] interface Vlan-interface 1
[5500-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

2. Perform Telnet-related configuration on the switch. Refer to “Telnet Configuration with Authentication Mode Being None” on page 53, “Console Port Login Configuration with Authentication Mode Being Password” on page 43, and “Telnet Configuration with Authentication Mode Being Scheme” on page 58 for more information.

3. Connect your PC/terminal and the switch to an Ethernet port, as shown in Figure 14. Make sure the port through which the switch is connected to the Ethernet belongs to VLAN 1 and the route between your PC and VLAN-interface 1 is reachable.

4. Launch Telnet on your PC, with the IP address of VLAN-interface 1 of the switch as the parameter, as shown in Figure 15.
If the password authentication mode is specified, enter the password when the Telnet window displays **Login authentication** and prompts for login password. The CLI prompt (such as <5500>) 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 series Ethernet switch can accommodate up to five Telnet connections at the same time.

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.

- **A Telnet connection is 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 “CLI Views” on page 24 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 16, 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 configure it.

**Figure 16** Network diagram for Telnetting to another switch from the current switch

1. Perform Telnet-related configuration on the switch operating as the Telnet server. Refer to “Telnet Configuration with Authentication Mode Being None” on page 53, “Configuring Telnet with the Password Authentication Mode” on page 55, and “Telnet Configuration with Authentication Mode Being Scheme” on page 58 for more.

2. Telnet to the switch operating as the Telnet client.

3. Execute the following command on the switch operating as the Telnet client:
<5500> telnet xxxx

Note that 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.

4 After successful login, the CLI prompt (such as <5500>) appears. If all the 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!**.

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.
LOGGING IN USING A MODEM

Introduction

The administrator can log into the console port of a remote switch using a modem through public switched telephone network (PSTN) if the remote switch is connected to the PSTN through a modem to configure and maintain the switch remotely. When a network operates improperly or is inaccessible, you can manage switches in the network remotely in this way.

To log into a switch in this way, you need to configure the administrator side and the switch properly, as listed in the following table.

Table 27  Requirements for logging into a switch using a modem

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator side</td>
<td>The PC can communicate with the modem connected to it.</td>
</tr>
<tr>
<td></td>
<td>The modem is properly connected to PSTN.</td>
</tr>
<tr>
<td></td>
<td>The telephone number of the switch side is available.</td>
</tr>
<tr>
<td>Switch side</td>
<td>The modem is connected to the console port of the switch properly.</td>
</tr>
<tr>
<td></td>
<td>The modem is properly configured.</td>
</tr>
<tr>
<td></td>
<td>The modem is properly connected to PSTN and a telephone set.</td>
</tr>
<tr>
<td></td>
<td>The authentication mode and other related settings are configured on the switch. Refer to Table 16.</td>
</tr>
</tbody>
</table>

Configuration on the Switch Side

Modem Configuration

Configure the modem that is directly connected to the switch using the following specifications:

AT&F  ---------------------- Restore the factory settings
AT&S0=1 ---------------------- Configure to answer automatically after the first ring
AT&D  ---------------------- Ignore DTR signal
AT&K0  ---------------------- Disable flow control
AT&R1  ---------------------- Ignore RTS signal
AT&S0  ---------------------- Set DSR to high level by force
ATEQ1&W  ---------------------- Disable the Modem from returning command response and the result, save the changes

You can verify your configuration by executing the AT&V command.

The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.
Switch Configuration

After logging into a switch through its console port by using a modem, you will enter the AUX user interface. The corresponding configuration on the switch is the same as those when logging into the switch locally through its console port except that:

- When you log in through the console port using a modem, the baud rate of the console port is usually set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.
- Other settings of the console port, such as the check mode, the stop bits, and the data bits, remain the default.

The configuration on the switch depends on the authentication mode the user is in. Refer to Table 16 for the information about authentication mode configuration.

Configuration on switch when the authentication mode is none
Refer to "Console Port Login Configuration with Authentication Mode Being None" on page 39.

Configuration on switch when the authentication mode is password
Refer to "Console Port Login Configuration with Authentication Mode Being Password" on page 43.

Configuration on switch when the authentication mode is scheme
Refer to "Console Port Login Configuration with Authentication Mode Being Scheme" on page 46.

Modem Connection Establishment

1. Before using a modem to log in to the switch, configure the different authentication modes on the switch. Refer to “Console Port Login Configuration with Authentication Mode Being None”, “Console Port Login Configuration with Authentication Mode Being Password”, and “Console Port Login Configuration with Authentication Mode Being Scheme” for more.

2. Perform the following configuration to the modem directly connected to the switch. Refer to “Modem Configuration” for related configuration.

3. Connect your PC, the modems, and the switch, as shown in Figure 17. Make sure the modems are properly connected to telephone lines.
Launch a terminal emulation utility on the PC and set the telephone number to call the modem directly connected to the switch, as shown in Figure 18 through Figure 20. Note that you need to set the telephone number to that of the modem directly connected to the switch.

**Figure 17** Establishing the connection using modems

4 Launch a terminal emulation utility on the PC and set the telephone number to call the modem directly connected to the switch, as shown in Figure 18 through Figure 20. Note that you need to set the telephone number to that of the modem directly connected to the switch.

**Figure 18** Create a connection
Figure 19  Set the telephone number

![Set the telephone number](image)

Figure 20  Call the modem

![Call the modem](image)

5 If the password authentication mode is specified, enter the password when prompted. If the password is correct, the prompt (such as <5500>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help.

> If you perform no AUX user-related configuration on the switch, the commands of level 3 are available to modem users. Refer to “CLI Configuration” on page 19 for information about the command line interface.
LOGGING IN THROUGH THE WEB-BASED NETWORK MANAGEMENT SYSTEM

Introduction

A Switch 5500 has a Web server built in. It enables you to log into a Switch 5500 through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log into a Switch 5500 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 28  Requirements for logging into a switch through the Web-based network management system

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>The VLAN interface of the switch is assigned an IP address, and the route between the switch and the Web network management terminal is reachable. (Refer to “IP Addressing Configuration” on page 123 and “IP Performance Configuration” on page 129.)</td>
</tr>
<tr>
<td></td>
<td>The user name and password for logging into the Web-based network management system are configured.</td>
</tr>
<tr>
<td>PC operating as the network management terminal</td>
<td>IE is available.</td>
</tr>
<tr>
<td></td>
<td>The IP address of the VLAN interface of the switch, the user name, and the password are available.</td>
</tr>
</tbody>
</table>

Establishing an HTTP Connection

1 Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch). See “Using Telnet to Connect from a Terminal to a Switch” for related information.

2 Configure the user name and the password on the switch for the Web network management user to log in.

# Create a Web user account, setting both the user name and the password to admin and the user level to 3.

```
<5500> system-view
[5500] local-user admin
[5500-luser-admin] service-type telnet level 3
[5500-luser-admin] password simple admin
```

3 Establish an HTTP connection between your PC and the switch, as shown in Figure 21.
CHAPTER 6: LOGGING IN THROUGH THE WEB-BASED NETWORK MANAGEMENT SYSTEM

Figure 21 Establish an HTTP connection between your PC and the switch

4 Log into 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 in the address bar. (Make sure the route between the Web-based network management terminal and the switch is available.)

5 When the login authentication interface (as shown in Figure 22) 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 22 The login page of the Web-based network management system

Configuring the Login Banner

Configuration Procedure

If a login banner is configured with the `header` command, when a user logs in through Web, the banner page is displayed before the user login authentication page. The contents of the banner page are the login banner information configured with the `header` command. Then, by clicking <Continue> on the banner page, the user can enter the user login authentication page, and enter the main page of the Web-based network management system after passing the authentication. If no login banner is configured by the `header` command, a user logging in through Web directly enters the user login authentication page.

Table 29 Configure the login banner

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the banner to be displayed when a user logs in through Web</td>
<td><code>header login text</code></td>
<td>Required By default, no login banner is configured.</td>
</tr>
</tbody>
</table>

Configuration Example

Network requirements

- A user logs in to the switch through Web.
- The banner page is desired when a user logs into the switch.
Enabling/Disabling the WEB Server

Figure 23  Network diagram for login banner configuration

![Network diagram](image)

Configuration Procedure

# Enter system view.

```
<5500> system-view
```

# Configure the banner **Welcome** to be displayed when a user logs into the switch through Web.

```
[5500] header login %Welcome%
```

Assume that a route is available between the user terminal (the PC) and the switch. After the above-mentioned configuration, if you enter the IP address of the switch in the address bar of the browser running on the user terminal and press <Enter>, the browser will display the banner page, as shown in Figure 24.

Figure 24  Banner page displayed when a user logs in to the switch through Web

![Banner page](image)

Click <Continue> to enter user login authentication page. You will enter the main page of the Web-based network management system if the authentication succeeds.

Enabling/Disabling the WEB Server

Follow the steps in Table 30 to enable or disable the Web server.

Table 30  Enable/Disable the WEB Server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
To improve security and prevent attack to the unused Sockets, TCP 80 port (which is for HTTP service) is enabled/disabled after the corresponding configuration.

- Enabling the Web server (by using the `undo ip http shutdown` command) opens TCP 80 port.
- Disabling the Web server (by using the `ip http shutdown` command) closes TCP 80 port.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the Web server</td>
<td><code>ip http shutdown</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the Web server is enabled.</td>
</tr>
<tr>
<td>Disable the Web server</td>
<td><code>undo ip http shutdown</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

Table 30  Enable/Disable the WEB Server
LOGGING IN THROUGH NMS

Introduction

You can also log into a switch through a network management station (NMS), and then configure and manage the switch through the agent module on the switch. Simple network management protocol (SNMP) is applied between the NMS and the agent. Refer to “SNMP Configuration” on page 795 and “RMON Configuration” on page 805 for related information.

To log into a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

Table 31  Requirements for logging into a switch through an NMS

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>The IP address of the VLAN interface of the switch is configured. The route between the NMS and the switch is reachable. (Refer to “IP Addressing Configuration” on page 123 and “IP Routing Protocol Overview” on page 277 for related information.) The basic SNMP functions are configured. (“SNMP Configuration” on page 795 and “RMON Configuration” on page 805 for related information.)</td>
</tr>
<tr>
<td>NMS</td>
<td>The NMS is properly configured. (Refer to the user manual of your NMS for related information.)</td>
</tr>
</tbody>
</table>

Connection Establishment Using NMS

Figure 25  Network diagram for logging in through an NMS
CONFIGURING SOURCE IP ADDRESSES FOR TELNET SERVICE PACKETS

Overview
You can configure the source IP address for Telnet service packets for a Switch 5500 unit operating as a Telnet client. The IP address can only be the IP address of a Layer 3 interface on the switch.

Figure 26 Specify source IP address for Telnet service packets

Figure 26 shows a telnet connection from a PC to Switch B. If devices in the segment 192.168.1.0/24 are not allowed to telnet to Switch B, you can log in to Switch A (a Switch 5500 Ethernet switch) first, configure the source IP address of the Telnet service packets on Switch A as 192.168.2.5, and then log in to Switch B through Switch A.

Configuring a Source IP Address for Telnet Service Packets
You can configure a source IP address for Telnet service packets in user view or in system view.

The configuration performed in user view takes effect for only the current session, while the configuration performed in system view takes effect for all of the following sessions. That is, when a switch telnets to a remote device, it automatically uses the configured source IP address or source interface to encapsulate Telnet service packets.

Table 32 describes how to configure a source IP address or source interface for service packs.

Table 32 Configuring a source IP address or source interface for service packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a source IP address or source interface for Telnet service packets for a Switch 5500 serving as a Telnet client</td>
<td>telnet { hostname</td>
<td>ip-address } [ service-port ] { source-ip ip-address</td>
</tr>
<tr>
<td></td>
<td>system-view telnet { source-ip ip-address</td>
<td>source-interface interface-type interface-number }</td>
</tr>
</tbody>
</table>

- The IP address specified is that of a Layer 3 interface of the local device. Otherwise, the system prompts configuration failure.
- The source interface specified must exist. Otherwise, the system prompts configuration failure.
- Configuring the source interface of Telnet service packets equals configuring the IP address of this interface as the source IP address of the Telnet service packets.
- If a source IP address (or source interface) is specified, you need to make sure that the route between the IP addresses (or interface) and the Telnet server is reachable.

### Displaying the Source IP Address Configuration

Execute the `display` command in any view to display the operation state after the above configurations. You can verify the configuration effect through the displayed information.

<table>
<thead>
<tr>
<th>Table 33</th>
<th>Displaying the source IP address configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Display the source IP address configured for the Telnet service packets</td>
<td><code>display telnet source-ip</code></td>
</tr>
</tbody>
</table>
Refer to “Password Control Configuration Operations” on page 957 for information about the ACL.

Introduction

You can control users logging in through Telnet, SNMP and WEB by defining Access Control List (ACL), as listed in Table 34.

Table 34  Controlling different types of login users

<table>
<thead>
<tr>
<th>Login mode</th>
<th>Control method</th>
<th>Implementation</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>By source IP address</td>
<td>Through basic ACL</td>
<td>“Controlling Telnet Users by Source IP Addresses”</td>
</tr>
<tr>
<td></td>
<td>By source and destination IP address</td>
<td>Through advanced ACL</td>
<td>“Controlling Telnet Users by Source and Destination IP Addresses”</td>
</tr>
<tr>
<td></td>
<td>By source MAC address</td>
<td>Through Layer 2 ACL</td>
<td>“Controlling Telnet Users by Source MAC Addresses”</td>
</tr>
<tr>
<td>SNMP</td>
<td>By source IP addresses</td>
<td>Through basic ACL</td>
<td>“Controlling Network Management Users by Source IP Addresses”</td>
</tr>
<tr>
<td>WEB</td>
<td>By source IP addresses</td>
<td>Through basic ACL</td>
<td>“Controlling Web Users by Source IP Address”</td>
</tr>
<tr>
<td></td>
<td>Disconnect Web users by force</td>
<td>By executing commands in CLI</td>
<td>“Disconnecting a Web User by Force”</td>
</tr>
</tbody>
</table>

Controlling Telnet Users

Prerequisites

Make sure to determine the control policy for Telnet users, including the source IP addresses, destination IP addresses, and source MAC addresses and the control actions (permitting or denying) you wish to implement.

Controlling Telnet Users by Source IP Addresses

Controlling Telnet users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 35  Control Telnet users by source IP addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Create a basic ACL or enter basic ACL view</td>
<td>`acl number acl-number [match-order {auto</td>
<td>config}]`</td>
</tr>
<tr>
<td>Define rules for the ACL</td>
<td>`rule [rule-id] {deny</td>
<td>permit} [rule-string]`</td>
</tr>
</tbody>
</table>
Controlling Telnet Users by Source and Destination IP Addresses

Controlling Telnet users by source and destination IP addresses is achieved by applying advanced ACLs, which are numbered from 3000 to 3999.

Table 35 Control Telnet users by source IP addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface [ type ] first-number [ last-number ]</td>
<td>-</td>
</tr>
<tr>
<td>Apply the ACL to control Telnet users by source IP addresses</td>
<td>acl acl-number { inbound</td>
<td>outbound }</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The `inbound` keyword specifies to filter the users trying to Telnet to the current switch.

The `outbound` keyword specifies to filter users trying to Telnet to other switches from the current switch.

Table 36 Control Telnet users by source and destination IP addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create an advanced ACL or enter advanced ACL view</td>
<td>acl number acl-number [ match-order { auto</td>
<td>config } ]</td>
</tr>
<tr>
<td>Define rules for the ACL</td>
<td>rule [ rule-id ] { deny</td>
<td>permit } protocol [ rule-string ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface [ type ] first-number [ last-number ]</td>
<td>-</td>
</tr>
<tr>
<td>Apply the ACL to control Telnet users by specified source and destination IP addresses</td>
<td>acl acl-number { inbound</td>
<td>outbound }</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The `inbound` keyword specifies to filter the users trying to Telnet to the current switch.

The `outbound` keyword specifies to filter users trying to Telnet to other switches from the current switch.

Controlling Telnet Users by Source MAC Addresses

Controlling Telnet users by source MAC addresses is achieved by applying Layer 2 ACLs, which are numbered from 4000 to 4999.

Table 37 Control Telnet users by source MAC addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create or enter Layer 2 ACL view</td>
<td>acl number acl-number</td>
<td>-</td>
</tr>
<tr>
<td>Define rules for the ACL</td>
<td>rule [ rule-id ] { deny</td>
<td>permit }</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>You can define rules as needed to filter by specific source MAC addresses.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 37  Control Telnet users by source MAC addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface [ type ]</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>first-number [ last-number ]</td>
<td>-</td>
</tr>
<tr>
<td>Apply the ACL to control Telnet users by specified source MAC addresses</td>
<td>acl acl-number inbound</td>
<td>Required By default, no ACL is applied for Telnet users.</td>
</tr>
</tbody>
</table>

### Configuration Example

**Network requirements**

Only the Telnet users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

**Network diagram**

*Figure 27  Network diagram for controlling Telnet users using ACLs*

1.110.100.46

Host A

1.110.100.52

Host B

IP network

Switch

### Configuration procedure

# Define a basic ACL.

```plaintext
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[5500-acl-basic-2000] quit
```

# Apply the ACL.

```plaintext
[5500] user-interface vty 0 4
[5500-ui-vty0-4] acl 2000 inbound
```

### Controlling Network Management Users by Source IP Addresses

You can manage a Switch 5500 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

Controlling network management users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 38 Control network management users by source IP addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Create a basic ACL or enter basic ACL view</td>
<td>`acl number acl-number [match-order {auto</td>
<td>config}]`</td>
</tr>
<tr>
<td>Define rules for the ACL</td>
<td>`rule [rule-id] {deny</td>
<td>permit} [rule-string]`</td>
</tr>
<tr>
<td>Quit to system view</td>
<td><code>quit</code></td>
<td>-</td>
</tr>
<tr>
<td>Apply the ACL while configuring the SNMP community name</td>
<td>`snmp-agent community [read</td>
<td>write] community-name [acl acl-number</td>
</tr>
<tr>
<td>Apply the ACL while configuring the SNMP group name</td>
<td>`snmp-agent group {v1</td>
<td>v2c} group-name [read-view</td>
</tr>
<tr>
<td>Apply the ACL while configuring the SNMP user name</td>
<td>`snmp-agent usm-user {v1</td>
<td>v2c} user-name group-name [acl acl-number]`</td>
</tr>
<tr>
<td></td>
<td>`snmp-agent usm-user v3 user-name group-name [cipher] [authentication-mode {md5</td>
<td>sha} auth-password [privacy-mode des56 priv-password] [acl acl-number]`</td>
</tr>
</tbody>
</table>

You can specify different ACLs while configuring the SNMP community name, SNMP group name, and SNMP user name.

As SNMP community name is a feature of SNMPv1 and SNMPv2c, the specified ACLs in the command that configures SNMP community names (the `snmp-agent community` command) take effect in the network management systems that adopt SNMPv1 or SNMPv2c.

Similarly, as SNMP group name and SNMP username name are a feature of SNMPv2c and the higher SNMP versions, the specified ACLs in the commands that configure SNMP group names and SNMP user names take effect in the network management systems that adopt SNMPv2c or higher SNMP versions. If you specify ACLs in the commands, the network management users are filtered by the SNMP group name and SNMP user name.
Controlling Web Users by Source IP Address

You can manage a Switch 5500 remotely through Web. Web users can access a switch through HTTP connections.

You need to perform the following two operations to control Web users by source IP addresses.

- Defining an ACL
- Applying the ACL to control Web users

Prerequisites

The controlling policy against Web users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Web Users by Source IP Addresses

Controlling Web users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Configuration Example

Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 are permitted to log into the switch.

Network diagram

Figure 28  Network diagram for controlling SNMP users using ACLs

![Network diagram](image-url)

Configuration procedure

# Define a basic ACL.

```
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[5500-acl-basic-2000] quit
```

# Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 to access the switch.

```
[5500] snmp-agent community read aaa acl 2000
[5500] snmp-agent group v2c groupa acl 2000
[5500] snmp-agent usm-user v2c usera groupa acl 2000
```
CHAPTER 9: USER CONTROL

Disconnecting a Web User by Force

The administrator can disconnect a Web user by force using the related commands.

### Table 39  Control Web users by source IP addresses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Create a basic ACL or enter basic ACL view</td>
<td>acl number acl-number [ match-order { config</td>
<td>auto } ]</td>
</tr>
<tr>
<td>Define rules for the ACL</td>
<td>rule [ rule-id ] { deny</td>
<td>permit } [ rule-string ]</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>Apply the ACL to control Web users</td>
<td>ip http acl acl-number</td>
<td>Optional By default, no ACL is applied for Web users.</td>
</tr>
</tbody>
</table>

### Configuration Example

Network requirements

Only the Web users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

**Figure 29**  Network diagram for controlling Web users using ACLs

Configuration procedure

# Define a basic ACL.

```
<5500> system-view
[5500] acl number 2030
[5500-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

# Apply ACL 2030 to only permit the Web users sourced from the IP address of 10.110.100.52 to access the switch.
[5500] ip http acl 2030
10

**Configuration File Management**

**Introduction to the Configuration File**

The configuration file records and stores user configurations performed on a switch. It also enables users to check switch configurations easily.

**Types of configuration**

You can configure a switch in two ways:

- To save the configuration used for initialization. If this file does not exist, the switch starts up without loading a configuration file.
- To use the current configuration, which refers to the user’s configuration during the switch’s operation. This configuration is stored in dynamic random-access memory (DRAM). It is removed when the switch is rebooted.

**Format of configuration file**

Configuration files are saved as text files for ease of reading. They:

- Save configuration in the form of commands.
- Save only non-default configuration settings.
- The commands are grouped into sections by command view. The commands that are of the same command view are grouped into one section. Sections are separated by comment lines. (A line is a comment line if it starts with the character `#`.)
- The sections are listed in this order: system configuration section, logical interface configuration section, physical port configuration section, routing protocol configuration section, user interface configuration, and so on.
- End with a return.

The operating interface provided by the configuration file management function is user-friendly. With it, you can easily manage your configuration files.

**Main/backup attribute of the configuration file**

Main and backup indicate the main and backup attribute of the configuration file respectively. A main configuration file and a backup configuration file can coexist on the switch. As such, when the main configuration file is missing or damaged, the backup file can be used instead. This increases the safety and reliability of the file system compared with the switch that only support one configuration file. You can configure a file to have both main and backup attribute, but only one file of either main or backup attribute is allowed on a switch.

The following three situations are concerned with the main/backup attributes:

- When saving the current configuration, you can specify the file to be a main or backup or normal configuration file.
CHAPTER 10: CONFIGURATION FILE MANAGEMENT

When removing a configuration file from a switch, you can specify to remove the main or backup configuration file. Or, if it is a file having both main and backup attribute, you can specify to erase the main or backup attribute of the file.

When setting the configuration file for next startup, you can specify to use the main or backup configuration file.

**Startup with the configuration file**
When booting, the system chooses the configuration files following the rules below:

1. If the main configuration file exists, the switch initializes with this configuration.
2. If the main configuration file does not exist but the backup configuration file exists, the switch initializes with the backup configuration.
3. If neither the main nor the backup configuration file exists, the switch starts up without loading the configuration file.

**Management of Configuration File**

**Table 41** Complete these tasks to configure configuration file management

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the current configuration</td>
<td>Optional</td>
</tr>
<tr>
<td>Erase the startup configuration file</td>
<td>Optional</td>
</tr>
<tr>
<td>Specify a configuration file for next startup</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Saving the Current Configuration**

You can modify the switch’s configuration using the command line interface (CLI). To use the modified configuration for your subsequent startups, you must save it (using the `save` command) as a configuration file.

**Table 42** Save current configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save current configuration</td>
<td><code>save [cfgfile][safely][backup][main]</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

**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 quicker but is likely to lose the original configuration file if the switch 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 slower but can retain the original configuration file in the switch even if the switch reboots or the power fails during the process.

**CAUTION:** The configuration file to be used for next startup may be lost if the switch reboots or the power fails during the configuration file saving process. In this case, the switch reboots without loading any configuration file. After the switch reboots, you need to specify a configuration file for the next startup. Refer to “Specifying a Configuration File for Next Startup” on page 90 for details.
Three attributes of the configuration file

- Main attribute. When you use the `save [ [ safely ] [ main ] ]` command to save the current configuration, the configuration file you get has main attribute. If this configuration file already exists and has backup attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its main attribute to allow only one main attribute configuration file in the switch.

- Backup attribute. When you use the `save [ safely ] backup` command to save the current configuration, the configuration file you get has backup attribute. If this configuration file already exists and has main attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its backup attribute to allow only one backup attribute configuration file in the switch.

- Normal attribute. When you use the `save cfgfile` command to save the current configuration, the configuration file you get has normal attribute if it is not an existing file. Otherwise, the attribute is dependent on the original attribute of the file.

3Com recommends that you adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.

- If you use the `save` command after a fabric is formed on the switch, the units in the fabric save their own startup configuration files automatically.

- The extension name of the configuration file must be `.cfg`.

Erasing the Startup Configuration File

You can clear the configuration files saved on the switch using the command in Table 43.

### Table 43 Erasing the configuration file

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase the startup configuration file from the storage switch</td>
<td>`reset saved-configuration [ backup</td>
<td>main ]`</td>
</tr>
</tbody>
</table>

You may need to erase the configuration file for one of these reasons:

- After you upgrade software, the old configuration file does not match the new software.
- The startup configuration file is corrupted or not the one you needed.

The following two situations exist:

- While the `reset saved-configuration [ main ]` command erases the configuration file with main attribute, it only erases the main attribute of a configuration file having both main and backup attribute.

- While the `reset saved-configuration backup` command erases the configuration file with backup attribute, it only erases the backup attribute of a configuration file having both main and backup attribute.
CAUTION: This command permanently deletes the configuration file from the switch.

Specifying a Configuration File for Next Startup

Use the following command to specify a configuration file for the next startup:

Table 44 Specify a configuration file for next startup

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a configuration file for</td>
<td>startup</td>
<td>Required</td>
</tr>
<tr>
<td>next startup</td>
<td>saved-configuration</td>
<td>Available in user view</td>
</tr>
<tr>
<td></td>
<td>`cfgfile [backup</td>
<td>main]`</td>
</tr>
</tbody>
</table>

You can specify a configuration file to be used for the next startup and configure the main/backup attribute for the configuration file.

Assign main attribute to the startup configuration file

- If you save the current configuration to the main configuration file, the system will automatically set the file as the main startup configuration file.
- You can also use the `startup saved-configuration cfgfile [backup | main]` command to set the file as main startup configuration file.

Assign backup attribute to the startup configuration file

- If you save the current configuration to the backup configuration file, the system will automatically set the file as the backup startup configuration file.
- You can also use the `startup saved-configuration cfgfile backup` command to set the file as backup startup configuration file.

CAUTION: The configuration file must use `.cfg` as its extension name and the startup configuration file must be saved at the root directory of the switch.

Displaying Device Configuration

After completing the above configuration, you can execute the `display` command in any view to display the current and initial configurations of the switch, so as to verify your configuration.
### Table 45  Display Device Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the initial configuration file saved in the switch’s flash memory</td>
<td><code>display saved-configuration [ unit unit-id ] [ by-linenum ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the configuration file used for this and next startup</td>
<td><code>display startup [ unit unit-id ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the switch’s current VLAN configuration</td>
<td><code>display current-configuration vlan [ vlan-id ] [ by-linenum ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the validated configuration in the current view</td>
<td><code>display this [ by-linenum ]</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display current configuration</td>
<td>`display current-configuration [ configuration [ configuration-type ]</td>
<td>interface [ interface-type ]</td>
</tr>
</tbody>
</table>
Introduction to XRN

Several XRN Switches of the same model can be interconnected to create a “Fabric”, in which each Switch is a unit. The ports used to interconnect all the units are called Fabric ports, while the other ports that are used to connect the Fabric to users are called user ports. In this way, you can increase ports and switching capability by adding devices to the Fabric. In addition, reliability of the system will be improved because the devices within the Fabric can backup each other. This feature brings you many advantages it:

- Provides unified management of multiple devices. Only one connection and one IP address are required to manage the entire Fabric. Therefore, management cost is reduced.
- Enables you to purchase devices on demand and expand network capacity smoothly. Protects your investment to the full extent during network upgrade.
- Ensures high reliability by N+1 redundancy, avoids single point failure, and lessens service interruption.

Figure 30  Fabric Example

Fabric Topology Mapper (FTM) function can manage and maintain Fabric topology. FTM on each unit exchanges information with other units, including unit ID, Fabric name, and the authentication mode between units, by using a special kind of protocol packets. It manages and maintains Fabric topology according to the acquired information. For example, when a new device is connected to a Fabric, FTM will determine whether it should establish a new Fabric with the device according to the information.
Configuring an XRN Fabric

FTM provides user interfaces. You can configure VLAN unit IDs, Fabric name, and the authentication mode between units by using the command.

### Table 46 Configuring FTM

<table>
<thead>
<tr>
<th>Device</th>
<th>Configuration</th>
<th>Default Settings</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>Specify the stacking VLAN of the Switch</td>
<td>The stacking VLAN is VLAN 4093</td>
<td>You should specify the stacking VLAN before the Fabric is established.</td>
</tr>
<tr>
<td></td>
<td>Set unit IDs for the Switches</td>
<td>The unit ID of a Switch is set to 1</td>
<td>Make sure that you have set different unit IDs to different Switches, so that the Fabric can operate normally after all the Switches are interconnected.</td>
</tr>
<tr>
<td></td>
<td>Specify the Fabric port of the Switch</td>
<td>-</td>
<td>For 28-port Switch, the 27th 28th port can be the Fabric port, for 52-port Switch, the 51st, 52nd port can be the Fabric port.</td>
</tr>
<tr>
<td></td>
<td>Set unit names for the Switches</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Set a name for the Fabric where the Switches belong</td>
<td>The Fabric name of the Switches is 5500</td>
<td>Interconnected the Switches with the same Fabric name to form a Fabric.</td>
</tr>
<tr>
<td></td>
<td>Set the authentication mode for the Fabric</td>
<td>No authentication mode is set on the Switches</td>
<td>Set the same authentication mode on all the devices within the Fabric.</td>
</tr>
</tbody>
</table>

The Switch 5500 Series: the SI units supports basic XRN, that is, Distributed Device Management (DDM) and Distributed Link Aggregation (DLA); the EI units support enhanced XRN, that is DDM, Distributed Resilient Routing (DRR).

### Specifying the Stacking VLAN of the Switch

You can use the command in the following table to specify the stacking VLAN of the Switch.

#### Table 47 Specifying the Stacking VLAN of the Switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the stacking VLAN of the Switch</td>
<td>ftm stacking-vlan vlan-id</td>
</tr>
<tr>
<td>Setting the stacking VLAN of the Switch to Default Value</td>
<td>undo ftm stacking-vlan</td>
</tr>
</tbody>
</table>

By default, the stacking VLAN is VLAN 4093.

You should specify the stacking VLAN before the Fabric is established.

### Setting Unit IDs for Switches

You can use the command in the following table to set unit IDs for Switches. Make sure to set different unit IDs for different Switches in a Fabric. On the Switches that support auto numbering, FTM will automatically number the Switches to constitute a Fabric, so that each Switch has a unique unit ID in the Fabric.

Perform the following configuration in System View.
### Configuring an XRN Fabric

Table 48  Setting unit IDs for Switches

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set unit IDs for Switches</td>
<td>`change unit-id &lt;1-8&gt; to {&lt;1-8&gt;</td>
</tr>
</tbody>
</table>

- If the modified unit ID does not exist in the Fabric, the Switch sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit ID is an existing one, the Switch prompts you to confirm if you really want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. Then you can use the `fabric save-unit-id` command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.
- If `auto-numbering` is selected, the system sets the unit ID priority to 10. You can use the `fabric save-unit-id` command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

The unit IDs in a Fabric are not necessarily numbered consecutively or in ascending order.

By default, the unit ID of a Switch is set to 1. A unit ID can be set to a value in the range from 1 to the maximum number of devices supported in XRN.

#### Saving the Unit ID of Each Unit in the Fabric

You can use the commands in the following table to save the unit ID of each unit in the Fabric to the unit Flash memory.

Table 49  Save the unit ID of each unit in the Fabric

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the unit ID of each unit in the fabric</td>
<td><code>fabric save-unit-id</code></td>
</tr>
<tr>
<td>Restore the unit ID of each unit in the fabric</td>
<td><code>undo fabric save-unit-id</code></td>
</tr>
</tbody>
</table>

#### Specifying the Fabric Port of the Switch

Perform the following configuration in System View.

Table 50  Specifying the Fabric Port of the Switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the stacking port of the Switch</td>
<td>`fabric-port { interface-name</td>
</tr>
<tr>
<td>cancel the stacking port of the Switch</td>
<td>`undo fabric-port { interface-name</td>
</tr>
</tbody>
</table>

For 28-port Switch, the ports 27 and 28 can be the Fabric port, for 52-port Switch, the ports 51 and 52 can be the Fabric port.

#### Setting Unit Names for Switches

You can use the command in the following table to set a unit name for each Switch.

Perform the following configuration in System View.
Setting a Fabric Name for Switches

Only the Switches with the same Fabric name and XRN authentication mode can constitute a Fabric.

You can use the commands in the following table to set a Fabric name for the Switches.

Perform the following configuration in System View.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set a Fabric name for Switches</td>
<td>sysname sysname</td>
</tr>
<tr>
<td>Restore the default Fabric name</td>
<td>undo sysname</td>
</tr>
</tbody>
</table>

By default, the Fabric name is “5500-EI”.

Setting an XRN Authentication Mode for Switches

Only the Switches with the same Fabric name and XRN authentication mode can constitute a Fabric.

You can use the commands in the following table to set an authentication mode for the Switches.

Perform the following configuration in System View.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set an XRN authentication mode for Switches</td>
<td>xrn-fabric authentication-mode { simple password</td>
</tr>
<tr>
<td>Restore the default XRN authentication mode</td>
<td>undo xrn-fabric authentication-mode</td>
</tr>
</tbody>
</table>

By default, no authentication mode is set on the Switches.

Displaying and Debugging a Fabric

Following completion of the above configuration, you can execute the display command in any view to view device management and verify the settings.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information of the entire Fabric</td>
<td>display xrn-fabric [ port ]</td>
</tr>
<tr>
<td>Display the topology information of Fabric</td>
<td>display ftm { information</td>
</tr>
</tbody>
</table>
Networking Requirements

Configure unit ID, unit name, Fabric name, and authentication mode for four Switches, and interconnect them to form a Fabric.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello
- Authentication mode: simple password
- Password: welcome

Networking Diagram

Figure 31  Networking Diagram of a Fabric

Configuration Procedure

Configure Switch A:

```
[SW5500] change unit-id 1 to 1
[SW5500] fabric-port gigabitethernet1/0/51 enable
[SW5500] fabric-port gigabitethernet1/0/52 enable
[SW5500] sysname hello
[hello] xrn-fabric authentication-mode simple welcome
```

Configure Switch B:

```
[SW5500] change unit-id 1 to auto-numbering
[SW5500] fabric-port gigabitethernet2/0/51 enable
[SW5500] fabric-port gigabitethernet2/0/52 enable
[SW5500] sysname hello
[hello] xrn-fabric authentication-mode simple welcome
```

Configure Switch C:

```
[SW5500] change unit-id 1 to auto-numbering
[SW5500] fabric-port gigabitethernet3/0/51 enable
[SW5500] fabric-port gigabitethernet3/0/52 enable
[SW5500] sysname hello
[hello] xrn-fabric authentication-mode simple welcome
```

Configure Switch D:
In the example, it is assumed that the system will automatically change the unit IDs of Switch B, Switch C and Switch D to 2, 3 and 4 after you choose auto-numbering for unit-id.

RMON on XRN

Interconnected switches form a fabric if they all support the XRN function and are all of the same type. The RMON configurations of the devices in a fabric are the same.

The RMON configuration performed on a device of a fabric will be automatically synchronized to all devices in the fabric if the configuration does not conflict with those of other devices in the fabric.

If you configure the same entry in the same ROM group for devices of a fabric to be different values, the entry values of all the conflicting devices will adopt that of the conflicting device with the smallest Unit ID when you synchronize the devices. Such a mechanism eliminates configuration conflicts between the devices in a fabric.

After the device configurations converge, you can collect RMON history and statistics data of any units from any switch in the fabric.

Configuration Commands for RMON on XRN

After the configurations of the switches in a fabric converge, you can use the following commands to collect RMON data of the devices in the fabric.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect the RMON statistics data</td>
<td><code>display rmon statistics unit</code></td>
<td>You can execute the <code>display rmon statistics unit</code> command in any view.</td>
</tr>
<tr>
<td>of a specified unit</td>
<td><code>unit-id</code></td>
<td></td>
</tr>
<tr>
<td>Collect the RMON history data</td>
<td><code>display rmon history unit</code></td>
<td></td>
</tr>
<tr>
<td>of a specified units</td>
<td><code>unit-id</code></td>
<td></td>
</tr>
</tbody>
</table>

Clustering on XRN

Through neighbor topology discovery protocol (NTDP), Clustering can collect the information about the connection relations of the devices in a network and candidate devices, consequently maintaining and managing the cluster topology.

With Clustering employed, the NTDP topology information collecting function is enabled by default on the management device of the cluster. And the timer is set to 1 minute. A management device can also perceive in time any changes of the cluster topology caused by new devices being added to the cluster and determine the candidate switches among the detected devices. By sending joining-request packets to candidate switches, the management device also enables these devices to be plug-and-play.
Peer Fabric Port Detection

As the basis of the XRN function, the fabric topology management (FTM) module manages and maintains the entire topology of a fabric. The FTM module also implements the peer fabric port detection function.

A device can join a fabric only when the following conditions are met.

- The number of the existing devices in the fabric does not reach the maximum number of devices allowed by the fabric.
- The fabric names of the device and the existing devices in the Fabric are the same.
- The software version of the device is the same as that of the existing devices in the fabric.
- The device passes the security authentication if security authentication is enabled in the fabric.

Work Flow of the Peer Fabric Port Detection Function

After a switch is powered on, the FTM module releases device information of the switch through the fabric ports. The device information includes UNIT ID, CPU MAC, device type ID, fabric port information, and all fabric configuration information. The device information is released in the form of discovery packet (DISC). A new device can join a fabric only when its DISC packets pass the authentication performed by the existing devices in the fabric.

- If a fabric port of a switch is connected to a non-fabric port, the switch will not receive DISC packets from the peer. In this case, the switch cannot join the fabric.
- If the switch can receive DISC packets sent by the peer, the FTM module determines whether peer sending ports correspond to local receiving ports according to information in the packet. That is, if a DISC packet received by the left port of the switch is sent by the right port of the peer device, the packet is regarded legal. Otherwise, the packet is regarded illegal and is discarded.
- If the maximum number of devices allowed by the fabric is reached, the devices in the fabric do not send DISC packets and discard the received DISC packets. This prevents new devices from joining the fabric.
- After receiving a DISC packet from a directly connected device, a device in a fabric checks whether the device information (that is, the Fabric name and software version) contained in the packet and those of its own are the same. If not, the received DISC packet is illegal and will be discarded.
- If authentication is enabled in the fabric, the current device in the fabric authenticates received packets sent by new directly connected devices. Packets that fail to pass the authentication will be discarded.

Prompt Information and Solution

normal

If the port displays "normal", it indicates the fabric operates properly.

temporary

If the port displays "temporary", it indicates the port status is changing.
redundance port

If the port displays "redundance port", it indicates the port is the redundant port in fabric ring topology.

*The "normal", "temporary" and "redundance port" information do not mean a device or a fabric operates improperly. No measure is needed for any of these three types of information.*

connection error

Analysis: The port matching errors (as listed in Table 56) may occur if a switch prompts the "connection error" message.

Solution: Take the measures listed in Table 56 accordingly.

Table 56 Connection error type and solution

<table>
<thead>
<tr>
<th>Error type</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two fabric ports of the same device (that is, the right port and the left port) are connected.</td>
<td>Pull out one end of the cable and connect it to a fabric port of another switch.</td>
</tr>
<tr>
<td>The left and right fabric ports of two devices are not connected in a crossed way.</td>
<td>Connect the left and right ports of two devices in a crossed way.</td>
</tr>
<tr>
<td>A fabric port of the local switch is connected to a non-fabric port.</td>
<td>Check the types of the two interconnected ports on two sides and make sure a fabric port is only connected to ports of the same type.</td>
</tr>
</tbody>
</table>

reached max units

Analysis: The "reached max units" message indicates that the maximum number of units allowed by the current fabric is reached. You will fail to add new devices to the fabric in this case.

Solution: Remove the new device or existing devices in the fabric.

*Up to eight devices can be in an XRN fabric at a time.*

different system name

Analysis: The "different system name" message indicates the fabric name of the device directly connected to the switch and the existing fabric name of the fabric are not the same. Only the devices with the same fabric name can form a Fabric.

Solution: Configure the fabric name of the new device to be that of the fabric.

different product version

Analysis: The "different product version" message indicates the software version of the directly connected device and that of the current device are not the same. A device can join a fabric only when its software version is identical to that of the fabric.

Solution: Make sure the software version of the new device is the same as that of the fabric.
auth failure

Analysis: The "auth failure" message indicates error occurs when the switch authenticates a directly connected device. The error may occur if the XRN fabric authentication modes configured for the both devices are not the same, or the password configured does not match.

Solution: Make sure the XRN fabric authentication modes and the passwords configured for the both devices are the same.

Multiple Fabric Port Candidates

On a Switch 5500 series switch, four GigabitEthernet ports can operate as fabric ports. The four ports are grouped into two groups. One group comprises of GigabitEthernet1/1/1 and GigabitEthernet1/1/2 ports, the other comprises of GigabitEthernet1/1/3 and GigabitEthernet1/1/4 ports. Only the ports of one group can operate as fabric ports at a time. Of the ports in the two groups, GigabitEthernet1/1/1 and GigabitEthernet1/1/3 ports can operate as UP fabric ports, and GigabitEthernet1/1/2 and GigabitEthernet1/1/4 ports can operates as DOWN fabric ports.

You can configure a port to be a fabric port using the **fabric port** command. Once you configure a port to be a fabric port, the group to which the port belongs becomes a fabric port group, and the other port in the group becomes a fabric port automatically. For example, after you configure the GigabitEthernet1/1/1 port to be a fabric port (a UP fabric port) by executing the **fabric port GigabitEthernet1/1/1 enable** command, the port group becomes a fabric port group, and GigabitEthernet1/1/2 port, which belongs to the same port group, becomes a DOWN fabric port.

*A port cannot be a fabric port if the jumboframe function is enabled on the port. So make sure the jumboframe function is disabled on a port if you want to configure the port to be a fabric port.*

With a port group of a switch being the current fabric port group, you need to invalidate the current fabric port group before configuring the other port group to be a fabric port group.

*After a fabric is configured, the master switch synchronizes its configuration file to all the units in the fabric. As the Flashes of the units may differ in size, the synchronizing operation may fail on certain units because of lack of Flash memory space, which makes the fabric fails to be established. So make sure each unit has enough free Flash memory space before configuring a fabric.*
VLAN Overview

Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.

- A switch is a link layer device which can forward a packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet.

The above scenarios could result in the following network problems.

- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.

- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.

Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

The virtual local area network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span across physical spaces. This enables hosts in a VLAN to be located in different physical locations.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help of network layer devices, such as routers and Layer 3 switches. Figure 32 illustrates a VLAN implementation.
Advantages of VLANs

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

- Broadcasts are confined to VLANs. This decreases bandwidth consumption and improves network performance.
- Network security is improved. Because each VLAN forms a broadcast domain, hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used.
- A more flexible way to establish virtual workgroups. VLAN can be used to create a virtual workgroup spanning physical network segments. When the physical position of a host changes within the range of the virtual workgroup, the host can access the network without changing its network configuration.

VLAN Principles

VLAN tags in the packets are necessary for a switch to identify packets of different VLANs. A switch works at the data link layer of the OSI model (Layer 3 switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you need to add the VLAN tag field into the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 33.

Figure 32 A VLAN implementation
In Figure 33 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the upper layer protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

**Figure 34** Format of VLAN tag

<table>
<thead>
<tr>
<th>DA&amp;SA</th>
<th>TPID</th>
<th>Priority</th>
<th>CFI</th>
<th>VLAN ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As shown in Figure 34, a VLAN tag contains four fields, including the tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in 3Com series Ethernet switches.
- Priority is a 3-bit field, referring to 802.1p priority. Refer to “QoS Configuration” on page 681 for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format. 0 (the value of the CFI filed) indicates the MAC address is encapsulated in the standard format and 1 indicates the MAC address is not encapsulated in the standard format. The value is 0 by default.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

The frame format here takes the Ethernet II encapsulation as an example. Ethernet also supports 802.2/802.3 encapsulation, where VLAN tag is also encapsulated after the DA and SA field. Refer to “Encapsulation Format of Ethernet Data” on page 108 for 802.2/802.3 encapsulation format.

VLAN ID identifies the VLAN to which a packet belongs. When a switch receives a packet carrying no VLAN tag, the switch encapsulates a VLAN tag with the default VLAN ID of the inbound port for the packet, and sends the packet to the default VLAN of the inbound port for transmission.

**MAC address learning mechanism of VLANs**

Switches forward packets according to the destination MAC addresses of the packets. So that switches maintain a table called MAC address forwarding table to record the source MAC addresses of the received packets and the corresponding ports receiving the packets for consequent packet forwarding. The process of recording is called MAC address learning.

After VLANs are configured on a switch, the MAC address learning of the switch has the following two modes.

- Shared VLAN learning (SVL): the switch records all the MAC address entries learnt by ports in all VLANs to a shared MAC address forwarding table. Packets received on any port of any VLAN are forwarded according to this table.
Independent VLAN learning (IVL): the switch maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received on a port of a VLAN is recorded to the MAC address forwarding table of this VLAN only, and packets received on a port of a VLAN are forwarded according to the VLAN's own MAC address forwarding table.

Currently, the 3Com Switch 5500 Family adopts the IVL mode only. For more information about the MAC address forwarding table, refer to “MAC Address Table Management” on page 209.

VLAN Interface

Hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used to do Layer 3 forwarding. The Switch 5500 Family supports VLAN interfaces configuration to forward packets in Layer 3.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the Layer 3 communication between different VLANs, and does not exist on a switch as a physical entity. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer. Normally, since VLANs can isolate broadcast domains, each VLAN corresponds to an IP network segment. And a VLAN interface serves as the gateway of the segment to forward packets in Layer 3 based on IP addresses.

VLAN Classification

Depending on how VLANs are established, VLANs fall into the following six categories.

- Port-based VLANs
- MAC address-based VLANs
- Protocol-based VLANs
- IP-subnet-based VLANs
- Policy-based VLANs
- Other types

At present, the Switch 5500 supports the port-based and protocol-based VLANs.

Port-Based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can assign the ports on the device to different VLANs. Thus packets received on a port will be transmitted through the corresponding VLAN only, so as to isolate hosts to different broadcast domains and divide them into different virtual workgroups.

Ports on Ethernet switches have the three link types: access, trunk, and hybrid. For the three types of ports, the process of being added into a VLAN and the way of forwarding packets are different. For details, refer to “Port Basic Configuration” on page 159.

Port-based VLANs are easy to implement and manage and applicable to hosts with relatively fixed positions.

Ethernet Port Link Types

A Switch 5500’s Ethernet port can operate using three link types:
Port-Based VLAN

- **Access**: An access port can belong to only one VLAN and is generally connected to a user’s PCs.
- **Trunk**: A trunk port can belong to more than one VLAN. It can receive and send packets from and to multiple VLANs and is generally connected to another switch.
- **Hybrid**: A hybrid port can belong to more than one VLAN. It can receive and send packets from and to multiple VLANs and is generally connected to either a switch or user’s PCs.

\[
\text{A hybrid port allows the packets of multiple VLANs to be sent untagged, but a trunk port only allows the packets of the default VLAN to be sent untagged.}
\]

The three types of ports can coexist on the same device.

### Assigning an Ethernet Port to Specific VLANs

You can assign an Ethernet port to a VLAN that forward packets for the VLAN, thus allowing the VLAN on the current switch to communicate with the same VLAN on the peer switch. You can assign an access port to only one VLAN, while you can assign a hybrid or trunk port to multiple VLANs.

\[
\text{Create the VLAN before assigning an access or hybrid port to that VLAN.}
\]

### Configuring the Default VLAN ID for a Port

An access port can belong to only one VLAN. Therefore, the VLAN to which an access port belongs is also the access port’s default VLAN. A hybrid or trunk port can belong to multiple VLANs, and so you should configure a default VLAN ID for the port.

After a port is added to a VLAN and configured with a default VLAN, the port receives and sends packets in a way related to its link type as described in Table 57, Table 58, and Table 59.

<table>
<thead>
<tr>
<th>Table 57</th>
<th>Access port packet processing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processing incoming packet</strong></td>
<td><strong>Processing an outgoing packet</strong></td>
</tr>
<tr>
<td><strong>For an Untagged Packet</strong></td>
<td><strong>For a Tagged Packet</strong></td>
</tr>
<tr>
<td>Receive the packet and add the default VLAN tag to the packet.</td>
<td>If the VLAN ID is just the default VLAN ID, receive the packet.</td>
</tr>
</tbody>
</table>
Protocol-Based VLAN

Introduction to Protocol-Based VLAN

Protocol-based VLAN is also known as protocol VLAN, which is another way to classify VLANs. Through the protocol-based VLANs, the switch can analyze the received packets carrying no VLAN tag on the port and match the packets with the user-defined protocol template automatically according to different encapsulation formats and the values of specific fields. If a packet is matched, the switch will add a corresponding VLAN tag to it automatically. Thus, data of specific protocol is assigned automatically to the corresponding VLAN for transmission.

This feature is used for binding the ToS provided in the network to VLAN to facilitate management and maintenance.

Encapsulation Format of Ethernet Data

This section introduces the common encapsulation formats of Ethernet data for you to understand well the procedure for the switch to identify the packet protocols.

---

Table 58  Trunk port packet processing

<table>
<thead>
<tr>
<th>Processing an incoming packet</th>
<th>Processing an outgoing packet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For an Untagged Packet</strong></td>
<td><strong>For a Tagged Packet</strong></td>
</tr>
<tr>
<td>If the port is already added to its default VLAN, add the default VLAN tag to the packet and then forward the packet. If the port is not added to its default VLAN, discard the packet.</td>
<td>If the VLAN ID is one of the VLAN IDs permitted to pass through the port, receive the packet. If the VLAN ID is not permitted to pass through the port, discard the packet.</td>
</tr>
<tr>
<td>If the VLAN ID is just the default VLAN ID, strip off the tag and send the packet. If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.</td>
<td></td>
</tr>
</tbody>
</table>

Table 59  Hybrid port packet processing

<table>
<thead>
<tr>
<th>Processing an incoming packet</th>
<th>Processing an outgoing packet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For an Untagged Packet</strong></td>
<td><strong>For a Tagged Packet</strong></td>
</tr>
<tr>
<td>If the port was already added to its default VLAN, add the default VLAN tag to the packet and then forward the packet. If the port was not added to its default VLAN, discard the packet.</td>
<td>If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.</td>
</tr>
<tr>
<td>Send the packet if the VLAN ID is allowed to pass through the port. Use the <code>port hybrid vlan</code> command to configure whether the port keeps or strips off the tags when sending VLAN packets (including the default VLAN).</td>
<td></td>
</tr>
</tbody>
</table>
**Ethernet II and 802.2/802.3 encapsulation**

Mainly, there are two encapsulation types of Ethernet packets: Ethernet II and 802.2/802.3, defined by RFC 894 and RFC 1042 respectively. The two encapsulation formats are described in the following figures.

Ethernet II packet:

**Figure 35**  Ethernet II encapsulation format

<table>
<thead>
<tr>
<th>DA&amp;SA(12)</th>
<th>Type(2)</th>
<th>Data</th>
</tr>
</thead>
</table>

802.2/802.3 packet:

**Figure 36**  802.2/802.3 encapsulation format

<table>
<thead>
<tr>
<th>DA&amp;SA(12)</th>
<th>Length(2)</th>
<th>DSAP(1)</th>
<th>SSAP(1)</th>
<th>Control(1)</th>
<th>OUI(3)</th>
<th>PID(2)</th>
<th>Data</th>
</tr>
</thead>
</table>

In the two figures, DA and SA refer to the destination MAC address and source MAC address of the packet respectively. The number in the bracket indicates the field length in bytes.

The maximum length of an Ethernet packet is 1500 bytes, that is, 0x05DC in hexadecimal, so the length field in 802.2/802.3 encapsulation is in the range of 0x0000 to 0x05DC.

Whereas, the type field in Ethernet II encapsulation is in the range of 0x0600 to 0xFFFF.

Packets with the value of the type or length field being in the range 0x05DD to 0x05FF are regarded as illegal packets and thus discarded directly.

The switch identifies whether a packet is an Ethernet II packet or an 802.2/802.3 packet according to the ranges of the two fields.

*The Switch 5500s recognize packets with the value of the type field being in the range 0x05DD to 0x05FF as 802.2/802.3 encapsulated packets.*

**Extended encapsulation formats of 802.2/802.3 packets**

802.2/802.3 packets have the following three extended encapsulation formats:

- 802.3 raw encapsulation: only the length field is encapsulated after the source and destination address field, followed by the upper layer data. No other fields are included.

**Figure 37**  802.3 raw encapsulation format

<table>
<thead>
<tr>
<th>DA&amp;SA(12)</th>
<th>Length(2)</th>
<th>Data</th>
</tr>
</thead>
</table>

Currently, only the IPX protocol supports 802.3 raw encapsulation, featuring with the value of the two bytes after the length field being 0xFFFF.
802.2 logical link control (LLC) encapsulation: the length field, the destination service access point (DSAP) field, the source service access point (SSAP) field and the control field are encapsulated after the source and destination address field. The value of the control field is always 3.

**Figure 38** 802.2 LLC encapsulation format

The DSAP field and the SSAP field in the 802.2 LLC encapsulation are used to identify the upper layer protocol. For example, if the two fields are both 0xE0, the upper layer protocol is IPX protocol.

802.2 sub-network access protocol (SNAP) encapsulation: encapsulates packets according to the 802.3 standard packet format, including the length, DSAP, SSAP, control, organizationally unique identifier (OUI), and protocol-ID (PID) fields.

**Figure 39** 802.2 SNAP encapsulation format

In 802.2 SNAP encapsulation format, the values of the DSAP field and the SSAP field are always 0xAA, and the value of the control field is always 3.

The switch differentiates between 802.2 LLC encapsulation and 802.2 SNAP encapsulation according to the values of the DSAP field and the SSAP field.

> When the OUI is 00-00-00 in 802.2 SNAP encapsulation, the PID field has the same meaning as the type field in Ethernet II encapsulation, which both refer to a globally unique protocol number. Such encapsulation is also known as SNAP RFC1042 encapsulation, which is standard SNAP encapsulation. The SNAP encapsulation mentioned in this chapter refers to SNAP RFC 1042 encapsulation.
Procedure for the Switch to Judge Packet Protocol

**Figure 40** Procedure for the switch to judge packet protocol

- **Receive packets**
- **Type(Length) field**
  - 0x0000 to 0x0600
  - 0x0600~0xFFFF

**Encapsulation Formats**

Table 60 lists the encapsulation formats supported by some protocols. In brackets are type values of these protocols.

**Table 60** Encapsulation formats

<table>
<thead>
<tr>
<th>Encapsulation Protocol</th>
<th>Ethernet II</th>
<th>802.3 raw</th>
<th>802.2 LLC</th>
<th>802.2 SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP (0x0800)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>IPX (0x8137)</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>AppleTalk (0x809B)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Implementation of Protocol-Based VLAN**

The Switch 5500 assigns the packet to the specific VLAN by matching the packet with the protocol template.

The protocol template is the standard to determine the protocol to which a packet belongs. Protocol templates include standard templates and user-defined templates:

- The standard template adopts the RFC-defined packet encapsulation formats and values of some specific fields as the matching criteria.
The user-defined template adopts the user-defined encapsulation formats and values of some specific fields as the matching criteria.

After configuring the protocol template, you must add a port to the protocol-based VLAN and associate this port with the protocol template. This port will add VLAN tags to the packets based on protocol types. The port in the protocol-based VLAN must be connected to a client. However, a common client cannot process VLAN-tagged packets. In order that the client can process the packets out of this port, you must configure the port in the protocol-based VLAN as a hybrid port and configure the port to remove VLAN tags when forwarding packets of all VLANs.
VLAN Configuration

Table 61  VLAN configuration tasks

<table>
<thead>
<tr>
<th>Configuration tasks</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic VLAN configuration</td>
<td>Required</td>
<td>“Basic VLAN Configuration”</td>
</tr>
<tr>
<td>Basic VLAN interface</td>
<td>Optional</td>
<td>“Basic VLAN Interface Configuration”</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Displaying VLAN</td>
<td>Optional</td>
<td>“Displaying VLAN Configuration”</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 62  Basic VLAN configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create multiple VLANs in</td>
<td>vlan {vlan-id \to\ vlan-id2</td>
<td>Optional</td>
</tr>
<tr>
<td>batch</td>
<td>all}</td>
<td></td>
</tr>
<tr>
<td>Create a VLAN and enter</td>
<td>vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td>VLAN view</td>
<td></td>
<td>By default, there is only one VLAN, that is, the default VLAN (VLAN 1).</td>
</tr>
<tr>
<td>Assign a name for the</td>
<td>name text</td>
<td>Optional</td>
</tr>
<tr>
<td>current VLAN</td>
<td></td>
<td>By default, the name of a VLAN is its VLAN ID. VLAN 0001, for example.</td>
</tr>
<tr>
<td>Specify the description</td>
<td>description</td>
<td>Optional</td>
</tr>
<tr>
<td>string of the current VLAN</td>
<td>text</td>
<td>By default, the description string of a VLAN is its VLAN ID. VLAN 0001,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for example.</td>
</tr>
</tbody>
</table>

CAUTION:

- **VLAN 1** is the system default VLAN, which needs not to be created and cannot be removed, either.

- The VLAN you created in the way described above is a static VLAN. On the switch, there are dynamic VLANs which are registered through GVRP. For details, refer to the chapter entitled “GVRP Configuration” on page 145.

- When you use the `vlan` command to create VLANs, if the destination VLAN is an existing dynamic VLAN, it will be transformed into a static VLAN and the switch will output the prompt information.
CHAPTER 13: VLAN CONFIGURATION

Basic VLAN Interface Configuration

Configuration prerequisites
Before configuring a VLAN interface, create the corresponding VLAN.

Configuration procedure

<table>
<thead>
<tr>
<th>Table 63</th>
<th>Basic VLAN interface configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>Create a VLAN interface and enter VLAN interface view</td>
<td><strong>interface Vlan-interface vlan-id</strong></td>
</tr>
<tr>
<td>Specify the description string for the current VLAN interface</td>
<td><strong>description text</strong></td>
</tr>
<tr>
<td>Disable the VLAN interface</td>
<td><strong>shutdown</strong></td>
</tr>
<tr>
<td>Enable the VLAN Interface</td>
<td><strong>undo shutdown</strong></td>
</tr>
</tbody>
</table>

*The operation of enabling/disabling a VLAN's VLAN interface does not influence the physical status of the Ethernet ports belonging to this VLAN.*

Displaying VLAN Configuration

<table>
<thead>
<tr>
<th>Table 64</th>
<th>Display VLAN configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Display the VLAN interface information</td>
<td><strong>display interface Vlan-interface</strong> [vlan-id]</td>
</tr>
<tr>
<td>Display the VLAN information</td>
<td><strong>display vlan</strong> [vlan-id [to vlan-id]]</td>
</tr>
<tr>
<td></td>
<td>all</td>
</tr>
</tbody>
</table>

Configuring a Port-Based VLAN

This section describes:

- Configuring an Ethernet Port’s Link Type
- Assigning an Ethernet Port to a VLAN
- Configuring the Default VLAN ID for a Port
- Displaying and Maintaining Port-Based VLAN
- Port-Based VLAN Configuration Example
Configuring a Port-Based VLAN

Configuring an Ethernet Port's Link Type

Follow these steps to configure an Ethernet port's link type.

Table 65  Configuring the Ethernet port's link type

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>--</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the port link type</td>
<td>port link-type {</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>access</td>
<td>hybrid</td>
</tr>
</tbody>
</table>

To change a port's link type from trunk to hybrid or from hybrid to trunk, you must first set the link type to access.

Assigning an Ethernet Port to a VLAN

You can assign an Ethernet port to a VLAN in Ethernet port view or in VLAN view.

In Ethernet port view

To assign an Ethernet port to one or multiple VLANs in Ethernet port view, use the commands in Table 66.

Table 66  Assigning an Ethernet port to a VLAN in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>--</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Assign the current port to one</td>
<td>port access vlan vlan-id</td>
<td>Optional</td>
</tr>
<tr>
<td>or multiple VLANs</td>
<td>port trunk permit vlan {</td>
<td>By default, all Ethernet ports belong to VLAN 1.</td>
</tr>
<tr>
<td></td>
<td>vlan-id-list</td>
<td>all }</td>
</tr>
<tr>
<td></td>
<td>port hybrid vlan vlan-id-list {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tagged</td>
<td>untagged }</td>
</tr>
</tbody>
</table>

When assigning an access or hybrid port to a VLAN, make sure the VLAN already exists.

In VLAN view

To assign an Ethernet port to one or multiple VLANs in in VLAN view, use the commands in Table 67.

Table 67  Assigning an ethernet port to a VLAN in VLAN view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system view</td>
<td>--</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the specified VLAN does not exist, this command creates the VLAN first.</td>
</tr>
<tr>
<td>Assign the specified access</td>
<td>port interface-list</td>
<td>Required</td>
</tr>
<tr>
<td>port or ports to the current</td>
<td></td>
<td>By default, all ports belong to VLAN 1.</td>
</tr>
<tr>
<td>VLAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Default VLAN for a Port

Because an access port can belong to only one VLAN, its default VLAN is the VLAN in which it resides. It cannot be configured. This section describes how to configure a default VLAN for a trunk or hybrid port.

To configure the default VLAN for a port, use the commands in Table 68.

Table 68  Configuring a port’s default VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>--</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the default VLAN for</td>
<td>port trunk pvid vlan</td>
<td>Optional</td>
</tr>
<tr>
<td>the current port</td>
<td>vlan-id</td>
<td></td>
</tr>
<tr>
<td>Hybrid port</td>
<td>port hybrid pvid vlan</td>
<td>The link type of a port is access</td>
</tr>
<tr>
<td></td>
<td>vlan-id</td>
<td>by default.</td>
</tr>
</tbody>
</table>

Caution: The local and remote trunk (or hybrid) ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

Displaying and Maintaining Port-Based VLAN

Network requirements

As shown in Figure 41, Switch A and Switch B connect to PC 1/PC 2 and Server 1/Server 2 used by different departments.

To isolate data between different departments, PC 1 and Server 1 are assigned to VLAN 100 with the descriptive string being Dept1; PC 2 and Server 2 are assigned to VLAN 200 with the descriptive string being Dept2.

Network diagram

Network diagram for a VLAN configuration on a Switch 5500.

Figure 41  Network diagram for VLAN configuration--Switch 5500
Configuration procedure

- Configure Switch A.

  # Create VLAN 100, specify its descriptive string as Dept1, and add Ethernet 1/0/1 to VLAN 100.

  <SwitchA> system-view
  [SwitchA] vlan 100
  [SwitchA-vlan100] description Dept1
  [SwitchA-vlan100] port Ethernet 1/0/1
  [SwitchA-vlan100] quit

- Configure Switch B.

  # Create VLAN 100, specify its descriptive string as Dept1, and add Ethernet 1/0/13 to VLAN 100.

  <SwitchB> system-view
  [SwitchB] vlan 100
  [SwitchB-vlan100] description Dept1
  [SwitchB-vlan100] port Ethernet 1/0/13
  [SwitchB-vlan103] quit

  # Create VLAN 200, specify its descriptive string as Dept2 and add Ethernet 1/0/11 and Ethernet 1/0/12 to VLAN 200.

  [SwitchB] vlan 200
  [SwitchB-vlan200] description Dept2
  [SwitchB-vlan200] port Ethernet 1/0/11 Ethernet 1/0/12
  [SwitchB-vlan200] quit

- Configure the link between Switch A and Switch B.

  Because the link between Switch A and Switch B needs to transmit data of both VLAN 100 and VLAN 200, you can configure the ports at both ends of the link as trunk ports and permit packets of the two VLANs to pass through the two ports.

  # Configure Ethernet 1/0/2 of Switch A.

  [SwitchA] interface Ethernet 1/0/2
  [SwitchA-Ethernet1/0/2] port link-type trunk
  [SwitchA-Ethernet1/0/2] port trunk permit vlan 100
  [SwitchA-Ethernet1/0/2] port trunk permit vlan 200

  # Configure Ethernet 1/0/10 of Switch B.

  [SwitchB] interface Ethernet 1/0/10
  [SwitchB-Ethernet1/0/10] port link-type trunk
  [SwitchB-Ethernet1/0/10] port trunk permit vlan 100
  [SwitchB-Ethernet1/0/10] port trunk permit vlan 200
CHAPTER 13: VLAN CONFIGURATION

Configuring a Protocol-Based VLAN

Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration tasks</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a protocol template for a protocol-based VLAN</td>
<td>Required</td>
<td>“Configuring a Protocol Template for a Protocol-Based VLAN”</td>
</tr>
<tr>
<td>Associating a port with a protocol-based VLAN</td>
<td>Required</td>
<td>“Associating a Port with a Protocol-Based VLAN”</td>
</tr>
<tr>
<td>Displaying protocol-based VLAN configuration</td>
<td>Optional</td>
<td>“Displaying Protocol-Based VLAN Configuration”</td>
</tr>
</tbody>
</table>

Configuration prerequisites

Create a VLAN before configuring the VLAN as a protocol-based VLAN.

Configuration procedure

Table 71  Configure the protocol template for a VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>—</td>
</tr>
<tr>
<td>Configure the protocol template for the VLAN</td>
<td>protocol-vlan [ protocol-index ] { at</td>
<td>ip</td>
</tr>
</tbody>
</table>

When configuring a protocol template for a protocol-based VLAN, use the at, ip or ipx keyword to configure a standard template to match AppleTalk, IP, and IPX packets respectively, and use the mode keyword to configure a user-defined template.

**CAUTION:**

- Because the IP protocol is closely associated with the ARP protocol, you are recommended to configure the ARP protocol type when configuring the IP protocol type and associate the two protocol types with the same port to avoid that ARP packets and IP packets are not assigned to the same VLAN, which will cause IP address resolution failure.

- If you specify some special values for both the dsap-id and ssap-id arguments when configuring the user-defined template for llc encapsulation, the matching packets will take the same encapsulation format as some standard type of packets. For example, when both dsap-id and ssap-id have a value of $0xFF$, the encapsulation format will be the same as that of ipx raw packets; if they both have a value of $0xE0$, the packet encapsulation format will be the same as that of ipx llc packets; if they both have a value of $0xAA$, the packet encapsulation format will be the same as that of snap packets. To prevent two commands from processing packets of the same protocol type in different
ways, the system does not allow you to set both the dsap-id and ssap-id arguments to 0xFF, 0xE0, or 0xAA.

- When you use the `mode` keyword to configure a user-defined protocol template, if you set the etype-id argument for `ethernetii` or `snap` packets to 0x0800, 0x8137, or 0x809B, the matching packets will take the same format as that of the IP, IPX, and AppleTalk packets respectively. To prevent two commands from processing packets of the same protocol type in different ways, the switch will prompt that you cannot set the etype-id argument for `Ethernet II` or `snap` packets to 0x0800, 0x8137, or 0x809B.

### Associating a Port with a Protocol-Based VLAN

#### Configuration prerequisites
- The protocol template for the protocol-based VLAN is configured.
- The port is configured as a hybrid port, and the port is configured to remove VLAN tags when it forwards the packets of the protocol-based VLANs.

#### Configuration procedure

**Table 72  Associate a port with the protocol-based VLAN**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td><code>-</code></td>
</tr>
<tr>
<td>Enter port view</td>
<td><code>interface interface-type interface-number</code></td>
<td><code>-</code></td>
</tr>
<tr>
<td>Associate the port with the specified protocol-based VLAN</td>
<td>`port hybrid protocol-vlan vlan vlan-id [ protocol-index [ to protocol-index-end ]</td>
<td>all ]`</td>
</tr>
</tbody>
</table>

**Table 73  Display protocol-based VLAN configuration**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about the protocol-based VLAN</td>
<td>`display vlan [ vlan-id [ to vlan-id ]</td>
<td>all</td>
</tr>
<tr>
<td>Display the protocol information and protocol indexes configured on the specified VLAN</td>
<td>`display protocol-vlan vlan { vlan-id [ to vlan-id ]</td>
<td>all }`</td>
</tr>
<tr>
<td>Display the protocol information and protocol indexes configured on the specified port</td>
<td>`display protocol-vlan interface { interface-type interface-number [ to interface-type interface-number ]</td>
<td>all ]`</td>
</tr>
</tbody>
</table>

#### Network requirements
- As shown in Figure 42, Workroom connects to the LAN through port Ethernet 1/0/10 on the Switch 5500.
- IP network and AppleTalk network workstations (hosts) coexist in the Workroom.
- The Switch 5500 connects to VLAN 100 (using IP network) through Ethernet 1/0/11 and to VLAN 200 (using AppleTalk network) through Ethernet 1/0/12.
Configure the switch to automatically assign the IP and AppleTalk packets to proper VLANs for transmission, so as to ensure the normal communication between the workstations and servers.

Network diagram

Figure 42  Network diagram for protocol-based VLAN configuration

![Network diagram](image)

Configuration procedure

# Create VLAN 100 and VLAN 200, and add Ethernet 1/0/11 and Ethernet 1/0/12 to VLAN 100 and VLAN 200 respectively.

```
<5500> system-view
[5500] vlan 100
[5500-vlan100] port Ethernet 1/0/11
[5500-vlan100] quit
[5500] vlan 200
[5500-vlan200] port Ethernet 1/0/12
```

# Configure protocol templates for VLAN 200 and VLAN 100, matching AppleTalk protocol and IP protocol respectively.

```
[5500-vlan200] protocol-vlan at
[5500-vlan200] quit
[5500] vlan 100
[5500-vlan100] protocol-vlan ip
```

# To ensure the normal operation of IP network, you need to configure a user-defined protocol template for VLAN 100 to match the ARP protocol (assume Ethernet II encapsulation is adopted here).

```
[5500-vlan100] protocol-vlan mode ethernetii etype 0806
```

# Display the created protocol-based VLANs and the protocol templates.

```
[5500-vlan100] display protocol-vlan vlan all
VLAN ID: 100
VLAN Type: Protocol-based VLAN
```
# Configure Ethernet 1/0/10 as a hybrid port, which removes the VLAN tag of the packets of VLAN 100 and VLAN 200 before forwarding the packets.

```
[5500-vlan100] quit
[5500] interface Ethernet 1/0/10
[5500-Ethernet1/0/10] port link-type hybrid
[5500-Ethernet1/0/10] port hybrid vlan 100 200 untagged
```

# Associate Ethernet1/0/10 with protocol template 0 and 1 of VLAN 100, and protocol template 0 of VLAN 200.

```
[5500-Ethernet1/0/10] port hybrid protocol-vlan vlan 100 0 to 1
[5500-Ethernet1/0/10] port hybrid protocol-vlan vlan 200 0
```

# Display the associations between Ethernet 1/0/10 and the VLAN protocol templates to verify your configuration.

```
[5500-Ethernet1/0/10] display protocol-vlan interface Ethernet 1/0/10
Interface: Ethernet1/0/10
<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Protocol-Index</th>
<th>Protocol-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0</td>
<td>ip</td>
</tr>
<tr>
<td>100</td>
<td>1</td>
<td>ethernetii etype 0x0806</td>
</tr>
<tr>
<td>200</td>
<td>0</td>
<td>at</td>
</tr>
</tbody>
</table>
```

The above output information indicates that Ethernet 1/0/10 has already been associated with the corresponding protocol templates of VLAN 100 and VLAN 200. Thus, packets from the IP and AppleTalk workstations can be automatically assigned to VLAN 100 and VLAN 200 respectively for transmission by matching the corresponding protocol templates, so as to realize the normal communication between workstations and servers.
IP Addressing
Overview

IP Address Classes
IP addressing uses a 32-bit address to identify each host on a network. 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.

For administration sake, IP addresses are divided into five classes, as shown in the following figure (in which the blue parts represent the address class).

Figure 43   IP address classes

<table>
<thead>
<tr>
<th>Class</th>
<th>0</th>
<th>7</th>
<th>15</th>
<th>23</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class B</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class C</td>
<td>110</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class D</td>
<td>1110</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class E</td>
<td>1111</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 74 describes the address ranges of these five classes. Currently, the first three classes of IP addresses are used in quantity.
CHAPTER 14: IP ADDRESSING CONFIGURATION

Special Case IP Addresses

The following IP addresses are for special use, and they cannot be used as host IP addresses:

- IP address with an all-zeros 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-zeros host ID: Identifies a network.
- IP address with an all-ones 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 section containing consecutive ones identifies the combination of net ID and subnet ID whereas the section containing consecutive zeros identifies the host ID.

Figure 44 shows how a Class B network is subnetted.

**Figure 44** Subnet a Class B network

<table>
<thead>
<tr>
<th>Class</th>
<th>Address range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.0.0.0 to 127.255.255.255</td>
<td>Address 0.0.0.0 means this host no this network. This address is used by a host at bootstrap when it does not know its IP address. This address is never a valid destination address. 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.</td>
</tr>
<tr>
<td>B</td>
<td>128.0.0.0 to 191.255.255.255</td>
<td>--</td>
</tr>
<tr>
<td>C</td>
<td>192.0.0.0 to 223.255.255.255</td>
<td>--</td>
</tr>
<tr>
<td>D</td>
<td>224.0.0.0 to 239.255.255.255</td>
<td>Multicast address.</td>
</tr>
<tr>
<td>E</td>
<td>240.0.0.0 to 255.255.255.255</td>
<td>Reserved for future use except for the broadcast address 255.255.255.255.</td>
</tr>
</tbody>
</table>
While allowing you to create multiple logical networks within a single Class A, B, or C network, subnetting is transparent to the rest of the Internet. All these networks still appear as one. As subnetting adds an additional level, subnet ID, to the two-level hierarchy with IP addressing, IP routing now involves three steps: delivery to the site, delivery to the subnet, and delivery to the host.

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 of 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-ones host ID is the broadcast address and the other with an all-zeros host ID is the network address) hosts before being subnets. 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 \((512 \cdot 126)\), 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

The Switch 5500 Family supports assigning IP addresses to VLAN interfaces and loopback interfaces. Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address 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.

This chapter only covers how to assign an IP address manually. For the other two approaches to IP address assignment, refer to “DHCP Overview” on page 597 and subsequent chapters.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>--</td>
</tr>
<tr>
<td>Enter interface view</td>
<td><code>interface</code></td>
<td><code>interface-type</code></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td><code>interface-number</code></td>
</tr>
<tr>
<td>Assign an IP address to the</td>
<td><code>ip address</code></td>
<td>Required</td>
</tr>
<tr>
<td>Interface</td>
<td>(p-address) { mask } [ sub ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mask-length</code></td>
<td></td>
</tr>
</tbody>
</table>

- You can assign at most five IP addresses to an interface for the Switch 5500 and seven IP addresses to an interface for the Switch 5500G, among which one is the primary IP address and the others are secondary IP addresses. A newly specified primary IP address overwrites the previous one if there is any.
- The primary and secondary IP addresses of an interface cannot reside on the same network segment; the IP address of a VLAN interface must not be on the same network segment as that of a loopback interface on a device.
- A VLAN interface cannot be configured with a secondary IP address if the interface has been configured to obtain an IP address through BOOTP or DHCP.
Displaying IP Addressing Configuration

After completing the above configuration, you can execute the `display` command in any view to display the operating status and configuration on the interface to verify your configuration.

### Table 76  Display IP addressing configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about a specified or all</td>
<td><code>display ip interface [interface-</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Layer 3 interfaces</td>
<td><code>type [interface-number]</code></td>
<td></td>
</tr>
<tr>
<td>Display brief configuration information about</td>
<td>`display ip interface brief [</td>
<td></td>
</tr>
<tr>
<td>a specified or all Layer 3 interfaces</td>
<td><code>interface-type [interface-</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>number ]</code></td>
<td></td>
</tr>
</tbody>
</table>

IP Address Configuration Examples

**IP Address Configuration Example I**

**Network requirement**

Assign IP address 129.2.2.1 with mask 255.255.255.0 to VLAN interface 1 of the switch.

**Network diagram**

**Figure 45  Network diagram for IP address configuration**

**Configuration procedure**

# Configure an IP address for VLAN interface 1.

```
<5500> system-view
[5500] interface Vlan-interface 1
[5500-Vlan-interface1] ip address 129.2.1.1 255.255.255.0
```

**IP Address Configuration Example II**

**Network requirements**

As shown in Figure 46, VLAN-interface 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 of the two networks.
Network diagram

Figure 46  Network diagram for IP address configuration

Configuration procedure

# Assign a primary IP address and a secondary IP address to VLAN-interface 1.

```plaintext
<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 the subnet 172.16.1.0/24, and to 172.16.2.1 on the PCs attached to the subnet 172.16.2.0/24.

# Ping a host on the subnet 172.16.1.0/24 from the switch to check the connectivity.

```plaintext
<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
```

```plaintext
--- 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 the switch can communicate with the hosts on the subnet 172.16.1.0/24.

# Ping a host on the 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 the switch can communicate with the hosts on the subnet 172.16.2.0/24.
**IP Performance Configuration**

**Introduction to IP Performance Configuration**

In some network environments, you need to adjust the IP parameters to achieve best network performance. The IP performance configuration supported by the Switch 5500 Family includes:

- Configuring TCP attributes
- Enabling reception of directed broadcasts to a directly connected network
- Disabling ICMP to send error packets

**Introduction to FIB**

Every switch stores a forwarding information base (FIB). FIB is used to store the forwarding information of the switch and guide Layer 3 packet forwarding.

You can know the forwarding information of the switch through the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the switch is running normally, the contents of the FIB and the routing table are the same.

### Configuring IP Performance Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure TCP attributes</td>
<td>Optional</td>
<td>“Configuring TCP Attributes”</td>
</tr>
<tr>
<td>Enable reception of directed broadcasts to a directly connected network</td>
<td>Optional</td>
<td>“Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network”</td>
</tr>
<tr>
<td>Disable ICMP to send error packets</td>
<td>Optional</td>
<td>“Disabling ICMP to Send Error Packets”</td>
</tr>
</tbody>
</table>

**Configuring TCP Attributes**

TCP optional parameters that can be configured include:

- **synwait timer**: When sending a SYN packet, TCP starts the synwait timer. If no response packets are received before the synwait timer times out, the TCP connection is not successfully created.
- **finwait timer**: When the TCP connection is changed into FIN_WAIT_2 state, finwait timer will be started. If no FIN packets are received within the timer timeout, the TCP connection will be terminated. If FIN packets are received, the TCP connection state changes to TIME_WAIT. If non-FIN packets are received, the system restarts the timer from receiving the last non-FIN packet. The connection is broken after the timer expires.

- **Size of TCP receive/send buffer**

**Table 78  Configure TCP attributes**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure TCP synwait timer’s timeout value</td>
<td>tcp timer syn-timeout time-value</td>
<td>Optional By default, the timeout value is 75 seconds.</td>
</tr>
<tr>
<td>Configure TCP finwait timer’s timeout value</td>
<td>tcp timer fin-timeout time-value</td>
<td>Optional By default, the timeout value is 675 seconds.</td>
</tr>
<tr>
<td>Configure the size of TCP receive/send buffer</td>
<td>tcp window window-size</td>
<td>Optional By default, the buffer is 8 kilobytes.</td>
</tr>
</tbody>
</table>

**Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network**

Directed broadcasts refer to broadcast packets sent to a specific network. In the destination IP address of a directed broadcast, the network ID is the ID of network where the receiving interface resides and the host ID is all-ones. Enabling the device to receive directed broadcasts will give hackers an opportunity to attack the network, thus bringing forth great potential dangers to the network.

By default, the Switch 5500 does not receive directed broadcast packets. You can configure the Switch 5500 to receive directed broadcast packets.

**Table 79  Enable the device to receive directed broadcasts**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the device to receive directed broadcasts</td>
<td>ip forward-broadcast</td>
<td>Required By default, the device is disabled from receiving directed broadcasts.</td>
</tr>
</tbody>
</table>

*After disabled from receiving directed broadcast to a directly connected network, the device discards all the directed broadcast data to that network.*

**Table 80  Enabling the device to forward directed broadcasts**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Enable the device to forward directed broadcasts</td>
<td>ip forward-broadcast [ acl-number ]</td>
<td>Required Disabled by default.</td>
</tr>
</tbody>
</table>
You can reference an ACL to forward only directed broadcasts permitted by the ACL.

If you execute the `ip forward-broadcast` command on an interface repeatedly, the last execution overwrites the previous one. If the command executed last time does not include the acl-number, the ACL configured previously will be removed.

Disabling ICMP to Send Error Packets

Sending error packets is a major function of ICMP protocol. 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.

Although sending ICMP error packets facilitate control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If receiving a lot of malicious packets that cause it to send ICMP error packets, the device’s performance will be reduced.
- As the ICMP 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.

You can disable the device from sending such ICMP error packets for reducing network traffic and preventing malicious attacks.

Table 81 Disable sending ICMP error packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Disable sending ICMP redirects</td>
<td><code>undo icmp redirect send</code></td>
<td>Required</td>
</tr>
<tr>
<td>Disable sending ICMP destination unreachable packets</td>
<td><code>undo icmp unreach send</code></td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>
## Displaying and Maintaining IP Performance Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display TCP connection status</td>
<td>display tcp status</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Display TCP connection statistics</td>
<td>display tcp statistics</td>
<td></td>
</tr>
<tr>
<td>Display UDP traffic statistics</td>
<td>display udp statistics</td>
<td></td>
</tr>
<tr>
<td>Display IP traffic statistics</td>
<td>display ip statistics</td>
<td></td>
</tr>
<tr>
<td>Display ICMP traffic statistics</td>
<td>display icmp statistics</td>
<td></td>
</tr>
<tr>
<td>Display the current socket information of the system</td>
<td>display ip socket [ socktype sock-type ] [ task-id socket-id ]</td>
<td></td>
</tr>
<tr>
<td>Display the forwarding information base (FIB) entries</td>
<td>display fib</td>
<td></td>
</tr>
<tr>
<td>Display the FIB entries matching the destination IP address</td>
<td>display fib ip_address1 [ { mask1</td>
<td>mask-length1 } ] ip_address2 { mask2</td>
</tr>
<tr>
<td>Display the FIB entries filtering through a specific ACL</td>
<td>display fib acl number</td>
<td></td>
</tr>
<tr>
<td>Display the FIB entries in the buffer which begin with, include or exclude the specified character string.</td>
<td>display fib [ { begin</td>
<td>include</td>
</tr>
<tr>
<td>Display the FIB entries filtering through a specific prefix list</td>
<td>display fib ip-prefix listname</td>
<td></td>
</tr>
<tr>
<td>Display the total number of the FIB entries</td>
<td>display fib statistics</td>
<td></td>
</tr>
<tr>
<td>Clear IP traffic statistics</td>
<td>reset ip statistics</td>
<td>You can execute the reset command in user view.</td>
</tr>
<tr>
<td>Clear TCP traffic statistics</td>
<td>reset tcp statistics</td>
<td></td>
</tr>
<tr>
<td>Clear UDP traffic statistics</td>
<td>reset udp statistics</td>
<td></td>
</tr>
</tbody>
</table>
Voice VLAN Overview

Voice VLANs are VLANs configured specially for voice traffic. By adding the ports connected with voice devices to voice VLANs, you can have voice traffic transmitted within voice VLANs and perform QoS-related configuration for voice traffic as required, thus ensuring the transmission priority of voice traffic and voice quality.

How an IP Phone Works

IP phones can convert analog voice signals into digital signals to enable them to be transmitted in IP-based networks. Used in conjunction with other voice devices, IP phones can offer large-capacity and low-cost voice communication solutions. As network devices, IP phones need IP addresses to operate properly in a network. An IP telephone can acquire an IP address automatically (as described here) or through manual configuration.

The following section describes a common way for an IP phone to acquire an IP address. The detailed process may vary by manufacture. Refer to the corresponding user manual for more detailed information.

When an IP phone applies for an IP address from a DHCP server, the IP phone can also apply for the following extensive information from the DHCP server through the Option184 field:

- IP address of the network call processor (NCP)
- IP address of the secondary NCP server
- Voice VLAN configuration
- Failover call routing

Refer to “DHCP Overview” on page 597 and subsequent DHCP chapters for more information.

Following describes the way an IP phone acquires an IP address.
As shown in Figure 47, the IP phone needs to work in conjunction with the DHCP server and the NCP to establish a path for voice data transmission. An IP phone goes through the following three phases to become capable of transmitting voice data.

1. After the IP phone is powered on, it sends an untagged DHCP request message containing four special requests in the Option 184 field besides the request for an IP address. The message is broadcast in the default VLAN of the receiving port. After receiving the DHCP request message, DHCP Server1, which resides in the default VLAN of the port receiving the message, responds as follows:
   - If DHCP Server1 does not support Option 184, it returns the IP address assigned to the IP phone but ignores the other four special requests in the Option 184 field. Without information about voice VLAN, the IP phone can only send untagged packets in the default VLAN of the port the IP phone is connected to. In this case, you need to manually configure the default VLAN of the port as a voice VLAN.
   - In cases where an IP phone obtains an IP address from a DHCP server that does not support Option 184, the IP phone directly communicates through the gateway after it obtains an IP address. It does not go through step 2 and step 3 described below.
   - If DHCP Server1 supports Option 184, it returns the IP address assigned to the IP phone, the IP address of the NCP, the voice VLAN ID, and so on.

2. On acquiring the voice VLAN ID from DHCP Server1, the IP phone ignores the IP address assigned by DHCP Server1 and sends a new DHCP request message carrying the voice VLAN tag to the voice VLAN. After receiving the DHCP request, DHCP Server2 residing in the voice VLAN assigns a new IP address to the IP phone and sends a tagged response message to the IP phone. After the IP phone receives the tagged response message, it sends voice data packets tagged with the voice VLAN tag. In this case, the port on the switch connecting to the IP phone must be configured to allow packets tagged with the voice VLAN tag to pass.
3 After the IP phone acquires the IP address assigned by DHCP Server2, the IP phone establishes a connection to the NCP specified by DHCP Server1 and downloads corresponding software. After that, the IP phone can communicate properly.

- An untagged packet carries no VLAN tag.
- A tagged packet carries the tag of a VLAN.

To set an IP address and a voice VLAN for an IP phone manually, just make sure that the voice VLAN ID to be set is consistent with that of the switch and the NCP is reachable to the IP address to be set.

How the Switch 5500 Identifies Voice Traffic

The Switch 5500 determines whether a received packet is a voice packet by checking its source MAC address. Packets with their source MAC addresses complying with the configured OUI (organizationally unique identifier) addresses are treated as voice packets. Ports receiving packets of this type will be added to the voice VLAN automatically for transmitting voice data.

You can configure OUI addresses for voice packets or specify to use the default OUI addresses.

An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address. The Switch 5500 supports OUI address mask configuration. You can adjust the matching depth of MAC address by setting different OUI address masks.

Table 83 lists the five default OUI addresses on the Switch 5500 Family.

<table>
<thead>
<tr>
<th>Number</th>
<th>OUI address</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0003-6b00-0000</td>
<td>Cisco phones</td>
</tr>
<tr>
<td>2</td>
<td>000f-e200-0000</td>
<td>3Com Aolynk phones</td>
</tr>
<tr>
<td>3</td>
<td>00d0-1e00-0000</td>
<td>Pingtel phones</td>
</tr>
<tr>
<td>4</td>
<td>00e0-7500-0000</td>
<td>Polycom phones</td>
</tr>
<tr>
<td>5</td>
<td>00e0-bb00-0000</td>
<td>3Com phones</td>
</tr>
</tbody>
</table>

Configuring Operation Mode for Voice VLAN

A voice VLAN can operate in two modes: automatic and manual. You can configure the operation mode for the voice VLAN according to data traffic passing through a port.

Processing mode of untagged packets sent by IP voice devices

- **Automatic mode.** A Switch 5500 automatically adds a port connecting an IP voice device to the voice VLAN by learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. The voice VLAN uses the aging mechanism to maintain the number of ports in the voice VLAN. When the aging timer expires, the ports whose OUI addresses are not updated (that is, no voice traffic passes) will be removed from the voice VLAN. In automatic mode, ports can not be added to or removed from a voice VLAN manually.
■ **Manual mode**: In this mode, you need to add a port to a voice VLAN or remove a port from a voice VLAN manually.

**Processing mode of tagged packets sent by IP voice devices**

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual mode is used.

**CAUTION**: If the voice traffic transmitted by an IP voice device carries VLAN tags, and 802.1x authentication and guest VLAN is enabled on the port which the IP voice device is connected to, assign different VLAN IDs for the voice VLAN, the default VLAN of the port, and the 802.1x guest VLAN to ensure the effective operation of these functions.

**Support for Voice VLAN on Various Ports**

Voice VLAN packets can be forwarded by access ports, trunk ports, and hybrid ports. You can enable a trunk or hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN.

For different types of IP phones, the support for voice VLAN varies with port types and port configuration. For IP phones capable of acquiring IP address and voice VLAN automatically, the support for voice VLAN is described in Table 84.

**Table 84  Matching relationship between port types and voice traffic types**

<table>
<thead>
<tr>
<th>Port voice VLAN mode</th>
<th>Voice traffic type</th>
<th>Port type</th>
<th>Supported or not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic mode</td>
<td>Tagged voice traffic</td>
<td>Access</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trunk</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hybrid</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Make sure the default VLAN of the port exists and is not a voice VLAN and the access port permits the traffic of the default VLAN.</td>
</tr>
<tr>
<td></td>
<td>Untagged voice traffic</td>
<td>Access</td>
<td>Not supported, because the default VLAN of the port must be a voice VLAN and the access port is in the voice VLAN. This can be done by adding the port to the voice VLAN manually.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hybrid</td>
<td></td>
</tr>
</tbody>
</table>
IP phones acquiring IP address and voice VLAN through manual configuration can forward only tagged traffic, so the matching relationship is relatively simple, as shown in Table 85.

### Table 85  Matching relationship between port types and voice devices

<table>
<thead>
<tr>
<th>Port voice VLAN mode</th>
<th>Port type</th>
<th>Supported or not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic mode</td>
<td>Access</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Trunk</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Hybrid</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN and the voice VLAN.</td>
</tr>
<tr>
<td>Manual mode</td>
<td>Access</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Trunk</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Hybrid</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN.</td>
</tr>
</tbody>
</table>

- **Tagged voice traffic**
  - **Access**: Make sure the default VLAN of the port exists and is not a voice VLAN and the access port permits the traffic of the default VLAN and the voice VLAN.
  - **Trunk**: Make sure that the default VLAN of the port exists and no a voice VLAN, and that the default VLAN and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.
  - **Hybrid**: Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose traffic is permitted by the access port.

- **Untagged voice traffic**
  - **Access**: Make sure the default VLAN of the port is a voice VLAN.
  - **Trunk**: Make sure the default VLAN of the port is a voice VLAN and the port permits the traffic of the VLAN.
  - **Hybrid**: Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose traffic is permitted by the port.
Voice VLAN Security Mode

On the Switch 5500, a voice VLAN can operate in the security mode and normal mode and is based on the filtering mechanisms of the voice VLAN-enabled ports on the inbound packets. In both modes, the voice VLAN-enabled ports process untagged packets and packets with the voice VLAN tags in different ways, as shown in step Table 86.

Table 86

<table>
<thead>
<tr>
<th>Voice VLAN mode</th>
<th>Inbound packet type</th>
<th>Processing method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security mode</td>
<td>Untagged packets</td>
<td>If the source MAC addresses of the packets are OUI addresses that can be identified by the system, send the packets to the voice VLAN; otherwise, discard the packets.</td>
</tr>
<tr>
<td></td>
<td>Packets with the voice VLAN tag</td>
<td></td>
</tr>
<tr>
<td>Normal mode</td>
<td>Untagged packets</td>
<td>The packet source MAC address will not be checked, and all packets can be transmitted in the voice VLAN.</td>
</tr>
<tr>
<td></td>
<td>Packets with the voice VLAN tag</td>
<td></td>
</tr>
</tbody>
</table>

In both modes, the port processes a packet with other VLAN tags in the same way, that is, it forwards the packet if the VLAN is allowed on the port and discards the packet if the VLAN is not allowed on the port.

3Com recommends that you do not mix voice packets with other types of data in a voice VLAN. If necessary, please ensure that the security mode is disabled.

Voice VLAN Configuration

Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- VLAN 1 (the default VLAN) cannot be configured as a voice VLAN.

Configuring a Voice VLAN to Operate in Automatic Mode

Table 87 Configure a voice VLAN to operate in automatic mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set an OUI address that can be identified by the voice VLAN</td>
<td>voice vlan mac-address oui mask oui-mask [ description text ]</td>
<td>Optional By default, the switch determines the voice traffic according to the default OUI address.</td>
</tr>
<tr>
<td>Enable the voice VLAN security mode</td>
<td>voice vlan security enable</td>
<td>Optional By default, the voice VLAN security mode is enabled.</td>
</tr>
<tr>
<td>Set the aging time for the voice VLAN</td>
<td>voice vlan aging minutes</td>
<td>Optional The default aging time is 1,440 minutes.</td>
</tr>
<tr>
<td>Enable the voice VLAN function globally</td>
<td>voice vlan vlan-id enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
</tbody>
</table>
CAUTION:

- For a voice VLAN operating in automatic mode, it only supports that the Hybrid port to process the tagged voice traffic. However, the protocol VLAN feature requires the Hybrid port to remove tags from the packets, see the VLAN section of this manual for details. Therefore, a VLAN cannot be configured as a voice VLAN and a protocol VLAN simultaneously.

- For a port operating in automatic mode, a default VLAN cannot be configured as a voice VLAN; otherwise the system prompts you for unsuccessful configuration.

When the voice VLAN is working normally, if the device restarts or the Unit ID of a device in an IRF fabric changes, in order to make the established voice connections work normally, the system does not need to be triggered by the voice traffic to add the port in automatic mode to the local devices as well as the IRF of the voice VLAN but does so immediately after the restart or the changes.

### Configuring a Voice VLAN to Operate in Manual Mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set an OUI address that can be identified by the voice VLAN</td>
<td>voice vlan mac-address oui mask oui-mask [ description text ]</td>
<td>Optional Without this address, the default OUI address is used.</td>
</tr>
<tr>
<td>Enable the voice VLAN security mode</td>
<td>voice vlan security enable</td>
<td>Optional By default, the voice VLAN security mode is enabled.</td>
</tr>
<tr>
<td>Set the aging time for a voice VLAN</td>
<td>voice vlan aging minutes</td>
<td>Optional The default aging time is 1,440 minutes.</td>
</tr>
<tr>
<td>Enable the voice VLAN function globally</td>
<td>voice vlan vlan-id enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enter port view</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
</tbody>
</table>
Table 88  Configure a voice VLAN to operate in manual mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable voice VLAN on a port</td>
<td>voice vlan enable</td>
<td>Required; By default, voice VLAN is disabled on a port.</td>
</tr>
<tr>
<td>Enable the voice VLAN legacy function on the port</td>
<td>voice vlan legacy</td>
<td>Optional; By default, voice VLAN legacy is disabled.</td>
</tr>
<tr>
<td>Set voice VLAN operation mode on a port to manual</td>
<td>undo voice vlan mode auto</td>
<td>Required; The default voice VLAN operation mode on a port is automatic.</td>
</tr>
</tbody>
</table>

Quit to system view

Add a port in manual mode to the voice VLAN

Access port

Enter VLAN view

Add the port to the VLAN

Trunk or Hybrid port

Enter port view

Add the port to the VLAN

Configure the voice VLAN to be the default VLAN of the port

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Required; By default, all the ports belong to VLAN 1.</td>
</tr>
<tr>
<td>port interface-list</td>
<td></td>
</tr>
<tr>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td>interface-num</td>
<td></td>
</tr>
<tr>
<td>port trunk permit vlan vlan-id</td>
<td>Optional; Refer to Table 84 to determine whether or not this operation is needed.</td>
</tr>
<tr>
<td>port hybrid vlan vlan-id { tagged</td>
<td>untagged }</td>
</tr>
<tr>
<td>port trunk pvid vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>port hybrid pvid vlan vlan-id</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:**

- The voice VLAN function can be enabled for only one VLAN at one time.
- If the Link Aggregation Control Protocol (LACP) is enabled on a port, voice VLAN feature cannot be enabled on it.
- Voice VLAN function can be enabled only for the static VLAN. A dynamic VLAN cannot be configured as a voice VLAN.
- When ACL number applied to a port reaches to its threshold, voice VLAN cannot be enabled on this port. You can use the `display voice vlan error-info` command to locate such ports.
- When a voice VLAN operates in security mode, the device in it permits only the packets whose source addresses are the identified voice OUI addresses. Packets whose source addresses cannot be identified, including certain authentication packets (such as 802.1x authentication packets), will be dropped. Therefore, you are suggested not to transmit both voice data and service data in a voice VLAN. If you have to do so, make sure that the voice VLAN does not operate in security mode.
The voice VLAN legacy feature realizes the communication between 3Com’s device and other vendor’s voice device by automatically adding the voice VLAN tag to the voice data coming from other vendors’ voice device. The voice_vlan legacy command can be executed before voice VLAN is enabled globally and on a port, but it takes effect only after voice VLAN is enabled globally and on the port.

To add a Trunk port or a Hybrid port to the voice VLAN, refer to the section entitled Port Basic Configurations in the 3Com Switch 5500 Family Command Reference Guide for the related command.

Displaying and Maintaining Voice VLAN

After completing the above configuration, you can execute the display command in any view to display the running status and verify the configuration using the commands in Table 89.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about ports on which voice VLAN configuration fails</td>
<td>display voice_vlan error-info</td>
<td>You can execute the display command in any view.</td>
</tr>
<tr>
<td>Display the voice VLAN configuration status</td>
<td>display voice_vlan status</td>
<td></td>
</tr>
<tr>
<td>Display the currently valid OUI addresses</td>
<td>display voice_vlan oui</td>
<td></td>
</tr>
<tr>
<td>Display the ports operating in the current voice VLAN</td>
<td>display vlan vlan-id</td>
<td></td>
</tr>
</tbody>
</table>

Voice VLAN Configuration Example

Network requirements
Create a voice VLAN and configure it to operate in automatic mode to enable the port to which an IP phone is connected to join or exit the voice VLAN automatically and voice traffic to be transmitted within the voice VLAN.

- Create VLAN 2 and configure it as a voice VLAN, with the aging time being 100 minutes.
- The IP phone sends tagged packets. It is connected to Ethernet 1/0/1, a hybrid port, with VLAN 6 being its default VLAN. Set this port to operate in automatic mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being test.
Network diagram

**Figure 48** Network diagram for voice VLAN configuration (automatic mode)

Configuration procedure

# Create VLAN 2 and VLAN 6.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 6
[DeviceA-vlan6] quit
```

# Set the aging time for the voice VLAN.

```
[DeviceA] voice vlan aging 100
```

# Add a user-defined OUI address 0011-2200-0000 and set the description string to test.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

# Enable the voice VLAN function globally.

```
[DeviceA] voice vlan 2 enable
```

# Configure the voice VLAN to operate in automatic mode on Ethernet 1/0/1. This operation is optional. By default, a voice VLAN operates in automatic mode on a port.

```
[DeviceA] interface Ethernet 1/0/1
[DeviceA-Ethernet1/0/1] voice vlan mode auto
```

# Configure Ethernet 1/0/1 as a hybrid port.

```
[DeviceA-Ethernet1/0/1] port link-type hybrid
```

# Configure VLAN 6 as the default VLAN of Ethernet 1/0/1, and configure Ethernet 1/0/1 to permit packets with the tag of VLAN 6.

```
[DeviceA-Ethernet1/0/1] port hybrid pvid vlan 6
[DeviceA-Ethernet1/0/1] port hybrid vlan 6 tagged
```

# Enable the voice VLAN function on Ethernet 1/0/1.
Voice VLAN Configuration Example (Manual Mode)

Network requirements
Create a voice VLAN and configure it to operate in manual mode. Add the port to which an IP phone is connected to the voice VLAN to enable voice traffic to be transmitted within the voice VLAN.

- Create VLAN 2 and configure it as a voice VLAN. Set the voice VLAN to operate in security mode.
- The IP phone sends untagged packets. It is connected to Ethernet 1/0/1, a hybrid port. Set this port to operate in manual mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being test.

Network diagram

Figure 49 Network diagram for voice VLAN configuration (manual mode)

- Device A
- VLAN 2
- Internet
- Device B
- 010-1001
- OUI 0011-2200-0000
- Mask ffff-ff00-0000

Configuration procedure

# Enable the security mode for the voice VLAN so that the ports in the voice VLAN permit valid voice packets only. This operation is optional. The security mode is enabled by default.
<DeviceA> system-view
[DeviceA] voice vlan security enable

# Add a user-defined OUI address 0011-2200-000 and set the description string to test.
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test

# Create VLAN 2 and configure it as a voice VLAN.
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] voice vlan 2 enable

# Configure Ethernet 1/0/1 to operate in manual mode.
[DeviceA] interface Ethernet 1/0/1
[DeviceA-Ethernet1/0/1] undo voice vlan mode auto
# Configure Ethernet 1/0/1 as a hybrid port.

[DeviceA-Ethernet1/0/1] port link-type hybrid

# Configure the voice VLAN as the default VLAN of Ethernet 1/0/1, and add the voice VLAN to the list of untagged VLANs whose traffic is permitted by the port.

[DeviceA-Ethernet1/0/1] port hybrid pvid vlan 2
[DeviceA-Ethernet1/0/1] port hybrid vlan 2 untagged

# Enable the voice VLAN function on Ethernet 1/0/1.

[DeviceA-Ethernet1/0/1] voice vlan enable

Verification

# Display the OUI addresses, the corresponding OUI address masks and the corresponding description strings that the system supports.

<DeviceA> display voice vlan oui

<table>
<thead>
<tr>
<th>Oui Address</th>
<th>Mask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0003-6b00-0000</td>
<td>ffff-ff00-0000</td>
<td>Cisco phone</td>
</tr>
<tr>
<td>000f-e200-0000</td>
<td>ffff-ff00-0000</td>
<td>3Com Aolynk phone</td>
</tr>
<tr>
<td>0011-2200-0000</td>
<td>ffff-ff00-0000</td>
<td>test</td>
</tr>
<tr>
<td>0040-1e00-0000</td>
<td>ffff-ff00-0000</td>
<td>Pingtel phone</td>
</tr>
<tr>
<td>00e0-7500-0000</td>
<td>ffff-ff00-0000</td>
<td>Polycom phone</td>
</tr>
<tr>
<td>00e0-bb00-0000</td>
<td>ffff-ff00-0000</td>
<td>3Com phone</td>
</tr>
</tbody>
</table>

# Display the status of the current voice VLAN.

<DeviceA> display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT MODE

----------------------------------------
Ethernet1/0/1 MANUAL
Introduction to GVRP

GVRP CONFIGURATION

GVRP VLAN registration protocol (GVRP) is an implementation of generic attribute registration protocol (GARP). GARP is introduced as follows.

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 bridged LAN the attributes specific to the GARP application, such as the VLAN or multicast attribute.

GARP itself does not exist on a device as an entity. GARP-compliant application entities are called GARP applications. One example is GVRP. When a GARP application entity is present on a port on your device, this port is regarded a GARP application entity.

GARP messages and timers

1 GARP messages

GARP members communicate with each other through the messages exchanged between them. The messages performing important functions for GARP fall into three types: Join, Leave and LeaveAll.

- When a GARP entity wants its attribute information to be registered on other devices, it sends Join messages to these devices. A GARP entity also sends Join messages when it receives Join messages from other entities or it wants some of its statically configured attributes to be registered on other GARP entities.

- When a GARP entity wants some of its attributes to be deregistered on other devices, it sends Leave messages to these devices. A GARP entity also sends Leave messages when it receives Leave messages from other entities for deregistering some attributes or it has some attributes statically deregistered.

- Once a GARP entity is launched, the LeaveAll timer is triggered at the same time. The GARP entity sends out LeaveAll messages after the timer times out. LeaveAll messages deregister all the attributes, through which the attribute information of the entity can be registered again on the other GARP entities.

Leave messages, LeaveAll messages, together with Join messages ensure attribute information can be deregistered and re-registered.

Through message exchange, all the attribute information to be registered can be propagated to all the GARP-enabled switches in the same LAN.

2 GARP timers
Timers determine the intervals of sending different types of GARP messages. GARP defines four timers to control the period of sending GARP messages.

- **Hold**: When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer and puts all received registration information before the timer times out into one Join message and sends out the message after the timer times out.

- **Join**: To make sure the devices can receive Join messages, each Join message is sent twice. If the first Join message sent is not responded for a specific period, a second one is sent. The period is determined by this timer.

- **Leave**: When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and deregisters the attribute information if it does not receives a Join message again before the timer times out.

- **LeaveAll**: Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveALL message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.

Unlike other three timers, which are set on a port basis, the LeaveAll timer is set in system view and takes effect globally.

A GARP application entity 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**

Through the mechanism of GARP, the configuration information on a GARP member will be propagated within the whole LAN. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/deregister its attribute information by declaration/recant, and register/deregister other GARP member's attribute information according to other member's declaration/recant. When a port receives an attribute declaration, the port will register this attribute. When a port receives an attribute recant, the port will deregister this attribute.

The protocol packets of GARP entities use specific multicast MAC addresses as their destination MAC addresses. When receiving these packets, the switch distinguishes them by their destination MAC addresses and delivers them to different GARP application (for example, GVRP) for further processing.

**GARP message format**

The GARP packets are in the following format:
Figure 50  Format of GARP packets

Table 90 describes the fields of a GARP packet.

Table 90  Description of GARP packet fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol ID</td>
<td>Protocol ID</td>
<td>1</td>
</tr>
<tr>
<td>Message</td>
<td>Each message consists of two parts: Attribute Type and Attribute List.</td>
<td>-</td>
</tr>
<tr>
<td>Attribute Type</td>
<td>Defined by the specific GARP application</td>
<td>The attribute type of GVRP is 0x01.</td>
</tr>
<tr>
<td>Attribute List</td>
<td>It contains multiple attributes.</td>
<td>-</td>
</tr>
<tr>
<td>Attribute</td>
<td>Each general attribute consists of three parts: Attribute Length, Attribute Event, and Attribute Value. Each LeaveAll attribute consists of two parts: Attribute Length and LeaveAll Event.</td>
<td>-</td>
</tr>
<tr>
<td>Attribute Length</td>
<td>The length of the attribute</td>
<td>2 to 255 (in bytes)</td>
</tr>
<tr>
<td>Attribute Event</td>
<td>The event described by the attribute</td>
<td>0: LeaveAll Event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1: JoinEmpty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2: JoinIn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3: LeaveEmpty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4: LeaveIn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5: Empty</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>The value of the attribute</td>
<td>For GVRP packets, the value of this field is the VLAN ID; however, for LeaveAll messages, this field is invalid.</td>
</tr>
<tr>
<td>End Mark</td>
<td>End mark of an GARP PDU</td>
<td>The value of this field is fixed to 0x00.</td>
</tr>
</tbody>
</table>
GVRP

As an implementation of GARP, GARP VLAN registration protocol (GVRP) maintains dynamic VLAN registration information and propagates the information to the other switches through GARP.

With GVRP enabled on a device, the VLAN registration information received by the device from other devices is used to dynamically update the local VLAN registration information, including the information about the VLAN members, the ports through which the VLAN members can be reached, and so on. The device also propagates the local VLAN registration information to other devices so that all the devices in the same LAN can have the same VLAN information. VLAN registration information propagated by GVRP includes static VLAN registration information, which is manually configured locally on each device, and dynamic VLAN registration information, which is received from other devices.

GVRP has the following three port registration modes: Normal, Fixed, and Forbidden, as described in the following.

- Normal. A port in this mode can dynamically register/deregister VLANs and propagate dynamic/static VLAN information.
- Fixed. A port in this mode cannot register/deregister VLANs dynamically. It only propagates static VLAN information. Besides, the port permits only static VLANs, that is, it propagates only static VLAN information to the other GARP members.
- Forbidden. A port in this mode cannot register/deregister VLANs dynamically. It permits only the default VLAN (namely, VLAN 1), that is, the port propagates only the information about VLAN 1 to the other GARP members.

Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

GVRP Configuration

GVRP Configuration Tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable GVRP</td>
<td>Required</td>
<td>“Enabling GVRP”</td>
</tr>
<tr>
<td>Configure GVRP timers</td>
<td>Optional</td>
<td>“Configuring GVRP Timers”</td>
</tr>
<tr>
<td>Configure GVRP port registration mode</td>
<td>Optional</td>
<td>“Configuring GVRP Port Registration Mode”</td>
</tr>
</tbody>
</table>

Enabling GVRP

Configuration Prerequisite

The port on which GVRP will be enabled must be set to a trunk port.

Configuration procedure

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
After you enable GVRP on a trunk port, you cannot change the port to a different type.

### Configuring GVRP Timers

<table>
<thead>
<tr>
<th>Table 92 Enable GVRP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enable GVRP globally</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
</tr>
<tr>
<td>Enable GVRP on the port</td>
</tr>
</tbody>
</table>

**Notes**

After you enable GVRP on a trunk port, you cannot change the port to a different type.

<table>
<thead>
<tr>
<th>Table 93 Configure GVRP timers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Configure the LeaveAll timer</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
</tr>
<tr>
<td>Configure the Hold, Join, and Leave timers</td>
</tr>
</tbody>
</table>

### Configuring GVRP Timers

- The setting of each timer must be a multiple of 5 (in centiseconds).
- The timer’s timeout ranges vary depending on the timeout values you set for other timers. If you want to set the a timer’s timeout time to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

Table 94 describes the relationships between the timers:

<table>
<thead>
<tr>
<th>Table 94 Timer relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timer</strong></td>
</tr>
<tr>
<td>Hold</td>
</tr>
</tbody>
</table>
CHAPTER 17: GVRP CONFIGURATION

In networking, the following GVRP timer settings are recommended:

- GARP hold timer: 100 centiseconds (1 second)
- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)
- GARP LeaveAll timer: 120000 centiseconds (2 minutes)

### Table 94 Timer relationships

<table>
<thead>
<tr>
<th>Timer</th>
<th>Lower threshold</th>
<th>Upper threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join</td>
<td>This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.</td>
<td>This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.</td>
</tr>
<tr>
<td>Leave</td>
<td>This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.</td>
<td>This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.</td>
</tr>
<tr>
<td>LeaveAll</td>
<td>This lower threshold is greater than the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.</td>
<td>32,765 centiseconds</td>
</tr>
</tbody>
</table>

In networking, the following GVRP timer settings are recommended:

- GARP hold timer: 100 centiseconds (1 second)
- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)
- GARP LeaveAll timer: 120000 centiseconds (2 minutes)

### Configuring GVRP Port Registration Mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure GVRP port</td>
<td>gvrp registration { fixed</td>
<td>Optional</td>
</tr>
<tr>
<td>registration mode</td>
<td>forbidden</td>
<td>normal }</td>
</tr>
</tbody>
</table>

### Displaying and Maintaining GVRP

After completing the above configuration, you can use the display command in any view to display the configuration information and operating status of GVRP/GARP, and thus verify your configuration. You can use the reset command in user view to clear GARP statistics.
GVRP Configuration Example

Network requirements

- Enable GVRP on all the switches in the network so that the VLAN configurations on Switch C and Switch E can be applied to all switches in the network, thus implementing dynamic VLAN information registration and refresh.
- By configuring the GVRP registration modes of specific Ethernet ports, you can enable the corresponding VLANs in the switched network to communicate with each other.

Network diagram

Figure 51  Network diagram for GVRP configuration

Configuration procedure for the Switch 5500

1  Configure Switch A

    # Enable GVRP globally.

    <SwitchA> system-view
    [SwitchA] gvrp

    # Configure Ethernet1/0/1 to be a trunk port and to permit the packets of all the VLANs.
# Enable GVRP on Ethernet1/0/1.

[SwitchA-Ethernet1/0/1] gvrp
[SwitchA-Ethernet1/0/1] quit

# Configure Ethernet1/0/2 to be a trunk port and to permit the packets of all the VLANs.

[SwitchA-Ethernet1/0/2] gvrp
[SwitchA-Ethernet1/0/2] quit

# Configure Ethernet1/0/3 to be a trunk port and to permit the packets of all the VLANs.

[SwitchA-Ethernet1/0/3] gvrp
[SwitchA-Ethernet1/0/3] quit

2 Configure Switch B

# The configuration procedure of Switch B is similar to that of Switch A and is thus omitted.

3 Configure Switch C

# Enable GVRP on Switch C, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5.

[SwitchC-vlan5] quit

4 Configure Switch D

# Enable GVRP on Switch D, which is similar to that of Switch A and is thus omitted.

# Create VLAN 8.

[SwitchD-vlan8] quit
5 Configure Switch E

# Enable GVRP on Switch E, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5 and VLAN 7.

[SwitchE] vlan 5
[SwitchE-vlan5] quit
[SwitchE] vlan 7
[SwitchE-vlan7] quit

6 Display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE] display vlan dynamic
Total 1 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  8

7 Configure Ethernet1/0/1 on Switch E to operate in fixed GVRP registration mode
and display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Configure Ethernet1/0/1 on Switch E to operate in fixed GVRP registration mode.

[SwitchE] interface Ethernet 1/0/1
[SwitchE-Ethernet1/0/1] gvrp registration fixed

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE-Ethernet1/0/1] display vlan dynamic
  No dynamic vlans exist!

8 Configure Ethernet1/0/1 on Switch E to operate in forbidden GVRP registration mode and display the VLAN registration information dynamically registered on Switch A, Switch B, and Switch E.

# Configure Ethernet1/0/1 on Switch E to operate in forbidden GVRP registration mode.

[SwitchE-Ethernet1/0/1] gvrp registration forbidden

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
  Total 2 dynamic VLAN exist(s).
  The following dynamic VLANs exist:
    5, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
  Total 2 dynamic VLAN exist(s).
  The following dynamic VLANs exist:
    5, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE] display vlan dynamic
  No dynamic vlans exist!

Configuration procedure for the Switch 5500

1 Configure Switch A

# Enable GVRP globally.

<SwitchA> system-view
[SwitchA] gvrp

# Configure GigabitEthernet1/0/1 to be a trunk port and to permit the packets of all the VLANs.

[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all

# Enable GVRP on GigabitEthernet1/0/1.

[SwitchA-GigabitEthernet1/0/1] gvrp
[SwitchA-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet1/0/2 to be a trunk port and to permit the packets of all the VLANs.

[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan all

# Enable GVRP on GigabitEthernet1/0/2.

[SwitchA-GigabitEthernet1/0/2] gvrp
[SwitchA-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet1/0/3 to be a trunk port and to permit the packets of all the VLANs.

[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan all

# Enable GVRP on GigabitEthernet1/0/3.

[SwitchA-GigabitEthernet1/0/3] gvrp
[SwitchA-GigabitEthernet1/0/3] quit

2 Configure Switch B

# The configuration procedure of Switch B is similar to that of Switch A and is thus omitted.

3 Configure Switch C

# Enable GVRP on Switch C, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5.

[SwitchC] vlan 5
[SwitchC-vlan5] quit

4 Configure Switch D

# Enable GVRP on Switch D, which is similar to that of Switch A and is thus omitted.

# Create VLAN 8.

[SwitchD] vlan 8
[SwitchD-vlan8] quit

5 Configure Switch E

# Enable GVRP on Switch E, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5 and VLAN 7.

[SwitchE] vlan 5
[SwitchE-vlan5] quit
CHAPTER 17: GVRP CONFIGURATION

6 Display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE] display vlan dynamic
Total 1 dynamic VLAN exist(s).
The following dynamic VLANs exist:
8

7 Configure GigabitEthernet1/0/1 on Switch E to operate in fixed GVRP registration mode and display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Configure GigabitEthernet1/0/1 on Switch E to operate in fixed GVRP registration mode.

[SwitchE] interface GigabitEthernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] gvrp registration fixed

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE-GigabitEthernet1/0/1] display vlan dynamic
No dynamic vlans exist!
8 Configure GigabitEthernet1/0/1 on Switch E to operate in forbidden GVRP registration mode and display the VLAN registration information dynamically registered on Switch A, Switch B, and Switch E.

# Configure GigabitEthernet1/0/1 on Switch E to operate in forbidden GVRP registration mode.

[SwitchE-GigabitEthernet1/0/1] gvrp registration forbidden

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 8,

# Display the VLAN information dynamically registered on Switch B.

[SwitchB] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 8,

# Display the VLAN information dynamically registered on Switch E.

[SwitchE] display vlan dynamic
No dynamic vlans exist!
# PORT BASIC CONFIGURATION

## Ethernet Port Overview

Table 97 lists the types and numbers of the ports on the 3Com Switch 5500.

### Table 97  Switch 5500 Family Hardware

<table>
<thead>
<tr>
<th>Switch 5500 Family</th>
<th>10BASE-T/100BASE-TX Ports</th>
<th>100BASE-T/1000BASE-TX/1000BASE-TX Ports</th>
<th>10BASE-X PoE Ports</th>
<th>100BASE-X SFP Ports</th>
<th>Stacking Ports</th>
<th>RJ-45 Console Port</th>
<th>48V DC RPS Input</th>
<th>Module Slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 5500-SI 28 Port</td>
<td>24</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500-SI 52 Port</td>
<td>48</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500-EI 28 Port</td>
<td>24</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500-EI 52 Port</td>
<td>48</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500 PWR 28 Port</td>
<td></td>
<td>24</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500 PWR 52 Port</td>
<td></td>
<td>48</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500 FX 28 Port</td>
<td>2</td>
<td>24</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500G-EI 24 Port</td>
<td>24</td>
<td>24†</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500G-EI 48 Port</td>
<td>48†</td>
<td>48†</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch 5500G-EI SFP 24 Port</td>
<td>4</td>
<td>24</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Depending on Power Supply Unit Fitted

†Combo SFP and 10/100/100 Ports
Each Combo optical port corresponds to an Ethernet electrical port, so there are four port pairs; only one port in a pair can be used at the same time. For the relationship between the Combo ports and the Ethernet ports, refer to Table 98.

**Table 98** Combo port list

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Combo Port</th>
<th>Corresponding port</th>
</tr>
</thead>
<tbody>
<tr>
<td>S5500-26Cor</td>
<td>25</td>
<td>22</td>
</tr>
<tr>
<td>S5500-26C-PWR</td>
<td>26</td>
<td>24</td>
</tr>
<tr>
<td>S5500-26</td>
<td>27</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>23</td>
</tr>
<tr>
<td>S5500-50C</td>
<td>49</td>
<td>46</td>
</tr>
<tr>
<td>S5500-50C-PWR</td>
<td>50</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>51</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>52</td>
<td>47</td>
</tr>
</tbody>
</table>

**Ethernet Port Configuration**

**Initially Configuring a Port**

Follow the steps in Table 99 to initially configure a port.

**Table 99** Initially configure a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><strong>interface</strong> interface-type</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td><strong>interface-number</strong></td>
<td>[182x425]</td>
</tr>
<tr>
<td>Enable the Ethernet port</td>
<td><strong>undo shutdown</strong></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the port is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <strong>shutdown</strong> command to disable the port.</td>
</tr>
<tr>
<td>Set the description string for the Ethernet port</td>
<td><strong>description</strong> text</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the description string of an Ethernet port is null.</td>
</tr>
<tr>
<td>Set the duplex mode of the Ethernet port</td>
<td><strong>duplex</strong> (auto</td>
<td>full</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the duplex mode of the port is <strong>auto</strong> (auto-negotiation).</td>
</tr>
<tr>
<td>Set the speed of the Ethernet port</td>
<td><strong>speed</strong> (speed-value</td>
<td>auto)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the speed of the port is <strong>auto</strong> (auto-negotiation).</td>
</tr>
<tr>
<td>Set the medium dependent interface (MDI) mode of the Ethernet port</td>
<td><strong>mdi</strong> { across</td>
<td>auto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Be default, the MDI mode of the port is <strong>auto</strong>. Currently, the devices do not support across or normal mode.</td>
</tr>
</tbody>
</table>
Configuring the Port’s Auto-Negotiation Speed

You can configure an auto-negotiation speed for a port by using the `speed auto` command.

Take a 10/100/1000 Mbps port as an example.

- If you expect that 10 Mbps is the only available auto-negotiation speed of the port, you just need to configure `speed auto 10`.
- If you expect that 10 Mbps and 100 Mbps are the available auto-negotiation speeds of the port, you just need to configure `speed auto 10 100`.
- If you expect that 10 Mbps and 1000 Mbps are the available auto-negotiation speeds of the port, you just need to configure `speed auto 10 1000`.

Follow the steps in Table 100 configure auto-negotiation speeds for a port.

<table>
<thead>
<tr>
<th>Table 100</th>
<th>Configure auto-negotiation speeds for a port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter Ethernet interface view</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>Configure the available auto-negotiation speed(s) for the port</td>
<td>`speed auto [10</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Only combo optical ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface card do not support this feature currently.
- After you configure auto-negotiation speed(s) for a port, if you execute the `undo speed` command or the `speed auto` command, the auto-negotiation speed setting of the port restores to the default setting.
- The effect of executing `speed auto 10 100 1000` equals to that of executing `speed auto`, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.

Limiting Traffic on Individual Ports

By performing the following configurations, you can limit different types of incoming traffic on individual ports. When a type of incoming traffic exceeds the threshold you set, the system drops the packets exceeding the traffic limit to
reduce the traffic ratio of this type to the reasonable range, so as to keep normal network service.

Follow the steps in Table 101 to limit the traffic on a port.

**Table 101  Limit traffic on port**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Limit broadcast traffic received on each port</td>
<td><code>broadcast-suppression</code> { ratio</td>
<td>pps max-pps }</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>broadcast-suppression</code> { ratio</td>
<td>pps max-pps }</td>
</tr>
<tr>
<td>Limit multicast traffic received on the current port</td>
<td><code>multicast-suppression</code> { ratio</td>
<td>pps max-pps }</td>
</tr>
<tr>
<td>Limit unknown unicast traffic received on the current port</td>
<td><code>unicast-suppression</code> { ratio</td>
<td>pps max-pps }</td>
</tr>
</tbody>
</table>

**Enabling Flow Control on a Port**

Flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch to stop sending packets to itself temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

Follow the steps in Table 102 to enable flow control on a port.

**Table 102  Enable flow control on a port**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Enable flow control on the Ethernet port</td>
<td><code>flow-control</code></td>
<td>By default, flow control is not enabled on the port.</td>
</tr>
</tbody>
</table>

**Copying a Port’s Configuration to Other Ports**

To make other ports have the same configuration as that of a specific port, you can duplicate the configuration of a port to specific ports.

Specifically, the following types of port configuration can be copied from one port to other ports: VLAN configuration, protocol-based VLAN configuration, LACP configuration, QoS configuration, GARP configuration, STP configuration and initial port configuration.
## Ethernet Port Configuration

- **VALN configuration**: includes IDs of the VLANs allowed on the port and the default VLAN ID of the port;
- **Protocol-based VLAN configuration**: includes IDs and indexes of the protocol-based VLANs allowed on the port;
- **Link aggregation control protocol (LACP) configuration**: includes LACP enable/disable status;
- **QoS configuration**: includes rate limit, port priority, and default 802.1p priority on the port;
- **Generic attribute registration protocol (GARP) configuration**: includes GVRP enable/disable status, timer settings, and registration mode;
- **STP configuration**: includes STP enable/disable status on the port, link attribute on the port (point-to-point or non-point-to-point), STP priority, path cost, packet transmission rate limit, whether loop protection is enabled, whether root protection is enabled, and whether the port is an edge port;
- **Port configuration**: includes link type of the port, port rate and duplex mode.

Follow the steps in Table 103 to duplicate the configuration of a port.

### Table 103  Duplicate the configuration of a port to specific ports

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Copy the configuration of a port to specific ports</td>
<td>copy configuration source { interface-type interface-number</td>
<td>aggregation-group source-agg-id } destination { interface-list [ aggregation-group destination-agg-id ]</td>
</tr>
</tbody>
</table>

- If you specify a source aggregation group ID, the system will use the port with the smallest port number in the aggregation group as the source.
- If you specify a destination aggregation group ID, the configuration of the source port will be copied to all ports in the aggregation group and all ports in the group will have the same configuration as that of the source port.

## Configuring Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if loopback occurs on a switch port.

After you enable loopback detection on Ethernet ports, the switch can monitor if external loopback occurs on them. If there is a loopback port found, the switch will put it under control.

- If loopback is found on an access port, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.
- If loopback is found on a trunk or hybrid port, the system sends a Trap message to the client. When the loopback port control function is enabled on these
ports, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.

Follow the steps in Table 104 to configure loopback detection for a port.

Table 104  Configure loopback detection for an Ethernet port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable loopback detection globally</td>
<td>loopback-detection enable</td>
<td>Required</td>
</tr>
<tr>
<td>Set the time interval for performing port loopback detection</td>
<td>loopback-detection interval-time time</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default interval is 30 seconds.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable loopback detection on a specified port</td>
<td>loopback-detection enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, port loopback detection is disabled.</td>
</tr>
<tr>
<td>Enable loopback port control on the trunk or hybrid port</td>
<td>loopback-detection control enable</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, loopback port control is not enabled.</td>
</tr>
<tr>
<td>Configure the system to run loopback detection on all VLANs of the current trunk or hybrid port</td>
<td>loopback-detection per-vlan enable</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the system runs loopback detection only on the default VLAN of the current trunk or hybrid port.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- To enable loopback detection on a specific port, you must use the `loopback-detection enable` command in both system view and the specific port view.

- After you use the `undo loopback-detection enable` command in system view, loopback detection will be disabled on all ports.

**Enabling Loopback Test**

You can configure the Ethernet port to run loopback test to check if it operates normally. The port running loopback test cannot forward data packets normally. The loopback test terminates automatically after a specific period.

Follow the steps in Table 105 to enable loopback testing.

Table 105  Enable loopback test

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure the Ethernet port to run loopback test</td>
<td>loopback { external</td>
<td>internal }</td>
</tr>
</tbody>
</table>
- **external**: Performs external loop test. In the external loop test, self-loop headers must be used on the port of the switch (for 1000M port, the self-loop header are made from eight cores of the 8-core cables, then the packets forwarded by the port will be received by itself.). The external loop test can locate the hardware failures on the port.

- **internal**: Performs internal loop test. In the internal loop test, self loop is established in the switching chip to locate the chip failure which is related to the port.

After you use the `shutdown` command on a port, the port cannot run loopback test. You cannot use the `speed`, `duplex`, `mdi` and `shutdown` commands on the ports running loopback test. Some ports do not support loopback test, and corresponding prompts will be given when you perform loopback test on them.

### Enabling the System to Test Connected Cable

You can enable the system to test the cable connected to a specific port. The test result will be returned in five seconds. The system can test these attributes of the cable: Receive and transmit directions (RX and TX), short circuit/open circuit or not, the length of the faulty cable.

Follow the steps in Table 106 to enable the system to test connected cables

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Enable the system to test connected cables</td>
<td><code>virtual-cable-test</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

Optical port (including Combo optical port) does not support VCT (`virtual-cable-test`) function.

*Combo electrical port supports VCT function only when it is in UP condition (using `undo shutdown` command), normal Ethernet electrical port always supports this function.*

### Configuring the Interval to Perform Statistical Analysis on Port Traffic

By performing the following configuration, you can set the interval to perform statistical analysis on the traffic of a port.

When you use the `display interface interface-type interface-number` command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set this interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input: 0 packets/sec 0 bytes/sec
Last 100 seconds output: 0 packets/sec 0 bytes/sec
```

Follow the steps in Table 107 to set the interval to perform a statistical analysis on port traffic.
CHAPTER 18: PORT BASIC CONFIGURATION

Enabling Giant-Frame Statistics Function

The giant-frame statistics function is used to ensure normal data transmission of network traffic and to facilitate statistics and analysis of unusual traffic on the network.

Follow the steps in Table 108 to enable the giant-frame statistics function.

Table 108 Enable the giant-frame statistics function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enable the giant-frame statistics</td>
<td>giant-frame statistics enable</td>
<td>Optional</td>
</tr>
<tr>
<td>function</td>
<td></td>
<td>By default, the giant-frame statistics function is not enabled</td>
</tr>
</tbody>
</table>

Configuring Storm Control on a Port

The storm control function is used to control traffic received on an Ethernet port.

- With traffic upper and lower thresholds specified on a port, the system periodically collects statistics about the broadcast/multicast/unicast/traffic on the port. Once it finds that a type of traffic exceeds the specified upper threshold, it blocks this type of traffic on the port or directly shuts down the port, and outputs trap/log information according to your configuration.

- When a type of traffic on the port falls back to the specified lower threshold, the system cancels the blocking of this type of traffic on the port or brings up the port to restore traffic forwarding for the port, and outputs log/trap information according to your configuration.

Follow the steps in Table 109 to configure storm control on a port.

Table 109 Configure storm control on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Set the upper and lower thresholds of broadcast/multicast/unicast traffic received on the port</td>
<td>storm-constrain {broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td>Set the action to be taken when a type of traffic received on the port exceeds the upper threshold.</td>
<td>storm-constrain control {block</td>
<td>shutdown }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no action is taken when a type of traffic reaches the upper threshold.</td>
</tr>
</tbody>
</table>
If the fabric function is enabled on a port of a device, you cannot configure the storm control function on all ports of the device.

If the broadcast-suppression command, multicast-suppression command or unicast suppression command is configured on a port, you cannot configure the storm control function on the port, and vice versa.

You are not recommended to set the upper and lower traffic thresholds to the same value.

If you specify the block keyword when executing the storm-constrain control command, only the packets beyond the upper thresholds are blocked when the overall traffic exceeds the upper threshold. In this case, the blocked packets are still taken into account when generating traffic statistics. If you specify the shutdown keyword when executing the command, the port will be shut down when the traffic passing through the port exceeds the upper threshold. You bring up the port again by executing the undo shutdown or the undo storm-constrain { all | broadcast | multicast | unicast } command.

Setting the Port State Change Delay

During a short period after you connect your switch to another device, the connecting port may go up and down frequently due to hardware compatibility, resulting in service interruption.

To avoid situations like this, you may introduce a port state change delay.

**Caution:** The port state change delay takes effect when the port goes down but not when the port goes up.

Follow the steps in Table 110 to set the port state change delay:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet interface view</td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Set the port state change delay</td>
<td>link-delay delay-time</td>
<td>Required</td>
</tr>
</tbody>
</table>

Defaults to 0, which indicates that no delay is introduced.
Displaying and Maintaining Basic Port Configuration

Follow the steps in Table 111 to display and maintain the basic port configuration.

Table 111 Display and maintain basic port configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display port configuration information</td>
<td>display interface [ interface-type interface-number ]</td>
<td>You can execute the display commands in any view.</td>
</tr>
<tr>
<td>Display the enable/disable status of port loopback detection</td>
<td>display loopback-detection</td>
<td></td>
</tr>
<tr>
<td>Display the information about the port with the link-delay command configured</td>
<td>display link-delay</td>
<td></td>
</tr>
<tr>
<td>Display brief information about port configuration</td>
<td>display brief interface [ interface-type interface-number ] [ { begin</td>
<td>include</td>
</tr>
<tr>
<td>Display Combo ports</td>
<td>display combo ports</td>
<td></td>
</tr>
<tr>
<td>Display the storm control configurations.</td>
<td>display storm-constrain [ interface interface-type interface-number ] [ { begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display port information about a specified unit</td>
<td>display unit unit-id interface</td>
<td></td>
</tr>
<tr>
<td>Display the statistics on the packets dropped packets</td>
<td>display packet-drop { interface [ interface-type interface-number ]</td>
<td>summary }</td>
</tr>
<tr>
<td>Clear port statistics</td>
<td>reset counters interface [ interface-type interface-number ]</td>
<td>You can execute the reset command in user view. After 802.1x is enabled on a port, clearing the statistics on the port will not work.</td>
</tr>
<tr>
<td>Clear the statistics on packets dropped on a port or all ports</td>
<td>reset packet-drop interface [ interface-type interface-number ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

Displaying and Clearing the Statistics on Dropped Packets

You can use the **display packet-drop** command in any view to display the statistics on the packets dropped on an Ethernet port and use the **reset packet-drop interface** command in user view to clear the statistics.

Table 112

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the statistics on dropped packets</td>
<td>display packet-drop { interface [ interface-type interface-number ]</td>
<td>summary }</td>
</tr>
<tr>
<td>Clear the statistics on dropped packets</td>
<td>reset packet-drop interface [ interface-type interface-number ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

The delay configured in this way does not take effect for ports in DLDP down state. For information about the DLDP down state, refer to DLDP.
Ethernet Port Configuration Example

Network requirements
■ Switch A and Switch B are connected to each other through two trunk port (Ethernet 1/0/1).
■ Configure the default VLAN ID of both Ethernet 1/0/1 to 100.
■ Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both Ethernet 1/0/1.

Network diagram
Figure 52 Network diagram for Ethernet port configuration

Configuration procedure
■ Only the configuration for Switch A is listed below. The configuration for Switch B is similar to that of Switch A.
■ This example supposes that VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 have been created.

# Enter Ethernet 1/0/1 port view.

<5500> system-view
[5500] interface ethernet 1/0/1

# Set Ethernet 1/0/1 as a trunk port.

[5500-Ethernet1/0/1] port link-type trunk

# Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass Ethernet 1/0/1.

[5500-Ethernet1/0/1] port trunk permit vlan 2 6 to 50 100

# Configure the default VLAN ID of Ethernet 1/0/1 to 100.

[5500-Ethernet1/0/1] port trunk pvid vlan 100

GigabitEthernet Port Configuration Example

Network requirements
■ Switch A and Switch B are connected to each other through two trunk port (GigabitEthernet 1/0/1).
■ Configure the default VLAN ID of both GigabitEthernet 1/0/1 to 100.
■ Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both GigabitEthernet 1/0/1.
Network diagram

Figure 53  Network diagram for Ethernet port configuration

Configuration procedure

- Only the configuration for Switch A is listed below. The configuration for Switch B is similar to that of Switch A.
- This example supposes that VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 have been created.

# Enter Ethernet port view of GigabitEthernet 1/0/1.

<5500G> system-view
System View: return to User View with Ctrl+Z.
[5500G] interface GigabitEthernet1/0/1

# Set GigabitEthernet1/0/1 as a trunk port.

[5500G-GigabitEthernet1/0/1] port link-type trunk

# Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass GigabitEthernet1/0/1.

[5500G-GigabitEthernet1/0/1] port trunk permit vlan 2 6 to 50 100

# Configure the default VLAN ID of GigabitEthernet1/0/1 to 100.

[5500G-GigabitEthernet1/0/1] port trunk pvid vlan 100

Troubleshooting Ethernet Port Configuration

Symptom: Fail to configure the default VLAN ID of an Ethernet port.

Solution: Take the following steps.

- Use the display interface or display port command to check if the port is a trunk port or a hybrid port.
- If the port is not a trunk or hybrid port, configure it to be a trunk or hybrid port.
- Configure the default VLAN ID of the port.
Overview

Introduction to Link Aggregation
Link aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

Link aggregation is designed to increase bandwidth by implementing load sharing among the member ports in an aggregation group. Link aggregation group also allows for port redundancy, which improves connection reliability.

Introduction to LACP
Link Aggregation Control Protocol (LACP) is designed to implement dynamic link aggregation and de aggregation. This protocol is based on IEEE802.3ad and uses link aggregation control protocol data units (LACPDUs) to interact with its peer.

With LACP enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

The system generates the operation key. It is determined by port settings such as port speed, duplex mode, and the basic configuration (refer to “Requirements on Ports for Link Aggregation” on page 171 for a description of the basic configurations).

- Selected ports in a manual aggregation group or a static aggregation group have the same operation key.
- Member ports in a dynamic aggregation group have the same operation key.

Requirements on Ports for Link Aggregation
To achieve load sharing in an aggregation group, the member ports to perform load balancing must have the same speed, duplex mode, and basic configurations, which include:

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, STP path cost, STP packet format, loop guard status, root guard status, edge port or not.
- QoS configuration, including traffic limit, priority remarking, 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID.
Link type configuration, which can be trunk, hybrid, or access.

GVRP configuration, including GVRP state (enabled/disabled), GVRP registration type, and GARP timer settings.

VLAN-VPN configuration, including VLAN-VPN state (enabled/disabled), Set the TPID value for the port, Enable the inner-to-outer tag priority replicating feature.

- The Switch 5500 supports cross-device link aggregation if IRF fabric is enabled.

<table>
<thead>
<tr>
<th>Link Aggregation Classification</th>
<th>Depending on different aggregation modes, the following three types of link aggregation exist:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual aggregation</td>
<td>Manual aggregation</td>
</tr>
<tr>
<td>Static LACP aggregation</td>
<td>Static LACP aggregation</td>
</tr>
<tr>
<td>Dynamic LACP aggregation</td>
<td>Dynamic LACP aggregation</td>
</tr>
</tbody>
</table>

**Manual Aggregation Group**

**Introduction to manual aggregation group**

A manual aggregation group is manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each manual aggregation group must contain at least one port. When a manual aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is disabled on the member ports of manual aggregation groups, and you cannot enable LACP on ports in a manual aggregation group.

**Port status in manual aggregation group**

A port in a manual aggregation group can be in one of the two states: selected or unselected. In a manual aggregation group, only the selected ports can forward user service packets.

In a manual aggregation group, the system sets the ports to selected or unselected state according to the following rules.

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected ports, and the rest are unselected ports.

- There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Among the selected ports in an aggregation group, the one with smallest port number operates as the master port. Other selected ports are the member ports.
Requirements on ports for manual aggregation

Generally, there is no limit on the rate and duplex mode of the ports (also including initially down port) you want to add to a manual aggregation group.

Static LACP Aggregation Group

Introduction to static LACP aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is enabled on the member ports of static aggregation groups. When you remove a static aggregation group, all the member ports in up state form one or multiple dynamic aggregations with LACP enabled. LACP cannot be disabled on static aggregation ports.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or unselected.

- Both the selected and the unselected ports can transceive LACP protocol packets.
- Only the selected ports can transceive service packets; the unselected ports cannot.

In a static aggregation group, the system sets the ports to selected or unselected state according to the following rules.

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected port, and the rest are unselected ports.
- The ports connected to a peer device different from the one the master port is connected to or those connected to the same peer device as the master port but to a peer port that is not in the same aggregation group as the peer port of the master port are unselected ports.
- The system sets the ports with basic port configuration different from that of the master port to unselected state.
- There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Dynamic LACP Aggregation Group

Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add or remove ports to or from it. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer
device and have the same speed, duplex mode, and basic configurations, and so are/do their peer ports.

Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

**Port status of dynamic aggregation group**

A port in a dynamic aggregation group can be in one of the two states: selected and unselected.

- Both the selected and the unselected ports in the “up” state can receive and transmit LACP protocol packets;
- The selected ports can receive/transmit user service packets, but the unselected ports cannot.
- In a dynamic aggregation group, the selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1. Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.

2. Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the selected port and the left ports are unselected ports.

   For an aggregation group:

   - When the rate or duplex mode of a port in the aggregation group changes, packet loss may occur on this port;
   - When the rate of a port decreases, if the port belongs to a manual or static LACP aggregation group, the port will be switched to the unselected state; if the port belongs to a dynamic LACP aggregation group, deaggregation will occur on the port.

### Aggregation Group Categories

Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups. When load sharing is implemented,

- For IP packets, the system will implement load-sharing based on source IP address and destination IP address;
For non-IP packets, the system will implement load-sharing based on source MAC address and destination MAC address.

In general, the system only provides limited load-sharing aggregation resources, so the system needs to reasonably allocate the resources among different aggregation groups.

The system always allocates hardware aggregation resources to the aggregation groups with higher priorities. When load-sharing aggregation resources are used up by existing aggregation groups, newly-created aggregation groups will be non-load-sharing ones.

Load-sharing aggregation resources are allocated to aggregation groups in the following order:

- An aggregation group containing special ports which require hardware aggregation resources has higher priority than any aggregation group containing no special port.
- A manual or static aggregation group has higher priority than a dynamic aggregation group (unless the latter contains special ports while the former does not).
- For aggregation groups, the one that might gain higher speed if resources were allocated to it has higher priority than others. If the groups can gain the same speed, the one with smallest master port number has higher priority than other groups.

When an aggregation group of higher priority appears, the aggregation groups of lower priorities release their hardware resources. For single-port aggregation groups, they can transceive packets normally without occupying aggregation resources.

**CAUTION:**

- A load-sharing aggregation group contains at least two selected ports, but a non-load-sharing aggregation group can only have one selected port at most, while others are unselected ports.
- When more than eight load-sharing aggregation groups are configured on a single switch, fabric ports cannot be enabled on this switch.
- When no more than eight load-sharing aggregation groups are configured on a single switch, fabric ports can be enabled on this switch. The aggregation groups added subsequently are all non-load-sharing aggregation groups. If the fabric ports are disabled, the state of these non-load-sharing aggregation groups will not be changed automatically. These non-load-sharing aggregation groups will become load-sharing aggregation groups only after the unselected ports in these aggregation groups are unplugged and then plugged or the `shutdown` command and then the `undo shutdown` command are executed.
CAUTION:

- The commands of link aggregation cannot be configured with the commands of port loopback detection feature at the same time.
- The ports where the `mac-address max-mac-count` command is configured cannot be added to an aggregation group. Contrarily, the `mac-address max-mac-count` command cannot be configured on a port that has already been added to an aggregation group.
- MAC-authentication-enabled ports and 802.1x-enabled ports cannot be added to an aggregation group.
- Mirroring destination ports and mirroring reflector ports cannot be added to an aggregation group.
- Ports configured with blackhole MAC addresses, static MAC addresses, multicast MAC addresses, or the static ARP protocol cannot be added to an aggregation group.
- Ports where the IP-MAC address binding is configured cannot be added to an aggregation group.
- Port-security-enabled ports cannot be added to an aggregation group.
- The port with Voice VLAN enabled cannot be added to an aggregation group.
- Do not add ports with the inter-VLAN MAC address replicating function of the selective QinQ feature enabled to an aggregation group.
- Do not add ports with IP filtering enabled to an aggregation group.
- Do not add ports with ARP intrusion detection enabled to an aggregation group.
- Do not add ports with source IP addresses/source MAC addresses statically bound to them to an aggregation group.
- Web-authentication-enabled ports cannot be added to an aggregation group.

Configuring a Manual Aggregation Group

You can create a manual aggregation group, or remove an existing manual aggregation group (after that, all the member ports will be removed from the group).

For a manual aggregation group, a port can only be manually added/removed to/from the manual aggregation group.

**Table 113** Configure a manual aggregation group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Create a manual aggregation group</td>
<td><code>link-aggregation group agg-id mode manual</code></td>
<td>Required</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Add the Ethernet port to the aggregation group</td>
<td><code>port link-aggregation group agg-id</code></td>
<td>Required</td>
</tr>
</tbody>
</table>
Note that:

1. When creating an aggregation group:
   - If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
   - If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
   - When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.

2. When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

**Configuring a Static LACP Aggregation Group**

You can create a static LACP aggregation group, or remove an existing static LACP aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or multiple dynamic aggregation groups.).

For a static aggregation group, a port can only be manually added/removed to/from the static aggregation group.

*When you add an LACP-enabled port to a manual aggregation group, the system will automatically disable LACP on the port. Similarly, when you add an LACP-disabled port to a static aggregation group, the system will automatically enable LACP on the port.*

**Table 114 Configure a static LACP aggregation group**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Create a static aggregation group</td>
<td>link-aggregation group agg-id mode static</td>
<td>Required</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Add the port to the aggregation group</td>
<td>port link-aggregation group agg-id</td>
<td>Required</td>
</tr>
</tbody>
</table>

*For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.*

**Configuring a Dynamic LACP Aggregation Group**

A dynamic LACP aggregation group is automatically created by the system based on LACP-enabled ports. The adding and removing of ports to/from a dynamic aggregation group are automatically accomplished by LACP.

You need to enable LACP on the ports which you want to participate in dynamic aggregation of the system, because, only when LACP is enabled on those ports at
both ends, can the two parties reach agreement in adding/removing ports to/from
dynamic aggregation groups.

You cannot enable LACP on a port which is already in a manual aggregation
group.

Table 115 Configure a dynamic LACP aggregation group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Configure the system priority</td>
<td><code>lacp system-priority</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><code>system-priority</code></td>
<td>By default, the system priority is 32,768.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type</code></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Enable LACP on the port</td>
<td><code>lacp enable</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, LACP is disabled on a port.</td>
</tr>
<tr>
<td>Configure the port priority</td>
<td><code>lacp port-priority</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><code>port-priority</code></td>
<td>By default, the port priority is 32,768.</td>
</tr>
</tbody>
</table>

Changing the system priority may affect the priority relationship between the
aggregation peers, and thus affect the selected/unselected status of member ports
in the dynamic aggregation group.

Perform the following tasks to configure a description for an aggregation group.

Table 116 Configure a description for an aggregation group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Configure a description for an aggregation group</td>
<td><code>link-aggregation group</code> agg-id <code>description</code> agg-name</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no description is configured for an aggregation group.</td>
</tr>
</tbody>
</table>

CAUTION: If you have saved the current configuration with the `save` command,
after system reboot, the configuration concerning manual and static aggregation
groups and their descriptions still exists, but that of dynamic aggregation groups
and their descriptions gets lost.

Displaying and Maintaining Link Aggregation Configuration

After completing the above configuration, you can execute the `display` command
in any view to display the running status after the link aggregation configuration
and verify your configuration. Execute the `reset` command in user view to clear
LACP statistics on ports.

Follow the steps in Table 117 to display and maintain link aggregation configuration.
Link Aggregation Configuration Example

**Network requirements**
- Switch A connects to Switch B with three ports Ethernet 1/0/1 to Ethernet 1/0/3. It is required that incoming/outgoing load between the two switches can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

**Network diagram**

*Figure 54* Network diagram for link aggregation configuration

---

**Table 117** Display and maintain link aggregation configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display summary information of all aggregation groups</td>
<td>display link-aggregation summary</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display detailed information of a specific aggregation group or all aggregation groups</td>
<td>display link-aggregation verbose [ agg-id ]</td>
<td></td>
</tr>
<tr>
<td>Display link aggregation details of a specified port or port range</td>
<td>display link-aggregation interface interface-type interface-number [ to interface-type interface-number ]</td>
<td></td>
</tr>
<tr>
<td>Display local device ID</td>
<td>display lacp system-id</td>
<td></td>
</tr>
<tr>
<td>Clear LACP statistics about a specified port or port range</td>
<td>reset lacp statistics [ interface interface-type interface-number [ to interface-type interface-number ] ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>
Configuration procedure

The following example only lists the configuration required on Switch A; you must perform the same configuration procedure on Switch B to implement link aggregation.

1 Adapting manual aggregation mode

# Create manual aggregation group 1.

<5500> system-view
[5500] link-aggregation group 1 mode manual

# Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] port link-aggregation group 1
[5500-Ethernet1/0/1] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port link-aggregation group 1
[5500-Ethernet1/0/2] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] port link-aggregation group 1

2 Adopting static LACP aggregation mode

# Create static aggregation group 1.

<5500> system-view
[5500] link-aggregation group 1 mode static

# Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] port link-aggregation group 1
[5500-Ethernet1/0/1] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port link-aggregation group 1
[5500-Ethernet1/0/2] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] port link-aggregation group 1

3 Adopting dynamic LACP aggregation mode

# Enable LACP on Ethernet 1/0/1 through Ethernet 1/0/3.

<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] lacp enable
[5500-Ethernet1/0/1] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] lacp enable
[5500-Ethernet1/0/2] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] lacp enable

CAUTION: The three LACP-enabled ports can be aggregated into one dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate, duplex mode, and so on).
PORT ISOLATION CONFIGURATION

Port Isolation Overview

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group. Thus, you can construct your network in a more flexible way and improve your network security.

Currently, you can create only one isolation group on the Switch 5500. The number of Ethernet ports in an isolation group is not limited.

- An isolation group only isolates the member ports in it.
- Port isolation is independent of VLAN configuration.

Port Isolation Configuration

You can perform the following operations to add an Ethernet port to an isolation group, thus isolating Layer 2 and Layer 3 data among the ports in the isolation group.

Table 118 Configure port isolation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type</code></td>
<td>—</td>
</tr>
<tr>
<td>Add the Ethernet port to the isolation group</td>
<td><code>port isolate interface-number</code></td>
<td>Required By default, an isolation group contains no port.</td>
</tr>
</tbody>
</table>

- When a member port of an aggregation group joins/leaves an isolation group, the other ports in the same aggregation group on the local unit will join/leave the isolation group at the same time.
- For ports that belong to an aggregation group and an isolation group simultaneously, removing a port from the aggregation group has no effect on the other ports. That is, the rest ports remain in the aggregation group and the isolation group.
- Ports that belong to an aggregation group and an isolation group simultaneously are still isolated even when you remove the aggregation group in system view.
- Adding a port of an isolation group to an aggregation group causes all the ports in the aggregation group being added to the isolation group.
- The Switch 5500 supports cross-device port isolation if IRF fabric is enabled.
- For Switch 5500s belonging to the same IRF Fabric, the port isolation configuration performed on a port of a cross-device aggregation group cannot
be synchronized to the other ports of the aggregation group if the ports reside on other units. That is, to add multiple ports in a cross-device aggregation group to the same isolation group, you need to perform the configuration for each of the ports individually.

Displaying and Maintaining Port Isolation Configuration

After completing the above configuration, you can execute the `display` command in any view to display the result of your port isolation configuration, thus verifying your configuration.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the Ethernet ports added to the isolation group</td>
<td><code>display isolate port</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
</tbody>
</table>

Network requirements

- PC2, PC3 and PC4 connect to the switch ports Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 ports.
- The switch connects to the Internet through Ethernet1/0/1.
- It is desired that PC2, PC3 and PC4 are isolated from each other so that they cannot communicate with each other.

Network diagram

![Network diagram for port isolation configuration](image)

Configuration procedure

# Add Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 to the isolation group.

```
<5500> system-view
System View: return to User View with Ctrl+Z.
```
Port Isolation Configuration Example

[5500] interface ethernet1/0/2
[5500-Ethernet1/0/2] port isolate
[5500-Ethernet1/0/2] quit
[5500] interface ethernet1/0/3
[5500-Ethernet1/0/3] port isolate
[5500-Ethernet1/0/3] quit
[5500] interface ethernet1/0/4
[5500-Ethernet1/0/4] port isolate
[5500-Ethernet1/0/4] quit
[5500] quit

# Display information about the ports in the isolation group.

<5500> display isolate port
Isolated port(s) on UNIT 1:
Ethernet1/0/2, Ethernet1/0/3, Ethernet1/0/4
Port Security
Overview

Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security allows you to define various security modes that enable devices to learn legal source MAC addresses, so that you can implement different network security management as needed.

With port security enabled, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets. The events that cannot pass 802.1x authentication or MAC authentication are considered illegal.

With port security enabled, upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

Port Security Features

The following port security features are provided:

- **NTK (need to know) feature**: By checking the destination MAC addresses in outbound data frames on the port, NTK ensures that the switch sends data frames through the port only to successfully authenticated devices, thus preventing illegal devices from intercepting network data.

- **Intrusion protection feature**: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on the port, intrusion protection detects illegal packets or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with the MAC address specified as illegal.

- **Trap feature**: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through the switch port, the Trap feature enables the switch to send Trap messages to help the network administrator monitor special activities.

Port Security Modes

Table 120 describes the available port security modes:
### Table 120 Description of port security modes

<table>
<thead>
<tr>
<th>Security mode</th>
<th>Description</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>noRestriction</td>
<td>In this mode, access to the port is not restricted.</td>
<td>In this mode, neither the NTK nor the intrusion protection feature is triggered.</td>
</tr>
<tr>
<td>autolearn</td>
<td>In this mode, the port automatically learns MAC addresses and changes them to security MAC addresses. This security mode will automatically change to the <code>secure</code> mode after the amount of security MAC addresses on the port reaches the maximum number configured with the <code>port-security max-mac-count</code> command. After the port security mode is changed to the <code>secure</code> mode, only those packets whose source MAC addresses are security MAC addresses learned or dynamic MAC addresses configured can pass through the port.</td>
<td>In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.</td>
</tr>
<tr>
<td>secure</td>
<td>In this mode, the port is disabled from learning MAC addresses. Only those packets whose source MAC addresses are security MAC addresses learned and static or dynamic MAC addresses can pass through the port.</td>
<td></td>
</tr>
<tr>
<td>userlogin</td>
<td>In this mode, port-based 802.1x authentication is performed for access users.</td>
<td>In this mode, neither NTK nor intrusion protection will be triggered.</td>
</tr>
</tbody>
</table>
Port Security Overview

### Table 120 Description of port security modes

<table>
<thead>
<tr>
<th>Security mode</th>
<th>Description</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>userLoginSecure</td>
<td>MAC-based 802.1x authentication is performed on the access user. The port is enabled only after the authentication succeeds. When the port is enabled, only the packets of the successfully authenticated user can pass through the port.</td>
<td>In any of these modes, the device triggers the NTK and Intrusion Protection features upon detecting an illegal packet or illegal event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>userLoginSecureExt</td>
<td>This mode is similar to the userLoginSecure mode, except that there can be more than one 802.1x-authenticated user on the port.</td>
<td></td>
</tr>
<tr>
<td>userLoginWithOUI</td>
<td>This mode is similar to the userLoginSecure mode, except that, besides the packets of the single 802.1x-authenticated user, the packets whose source MAC addresses have a particular OUI are also allowed to pass through the port.</td>
<td></td>
</tr>
<tr>
<td>macAddressWithRadiusius</td>
<td>In this mode, MAC address-based authentication is performed for access users.</td>
<td></td>
</tr>
<tr>
<td>macAddressOrUserLoginSecure</td>
<td>In this mode, both MAC authentication and 802.1x authentication can be performed, but 802.1x authentication has a higher priority. 802.1x authentication can still be performed on an access user who has passed MAC authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No MAC authentication is performed on an access user who has passed 802.1x authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users.</td>
<td></td>
</tr>
<tr>
<td>macAddressOrUserLoginSecureExt</td>
<td>This mode is similar to the macAddressOrUserLoginSecure mode, except that there can be more than one 802.1x-authenticated user on the port.</td>
<td></td>
</tr>
</tbody>
</table>
When the port operates in the userlogin-withoui mode, Intrusion Protection will not be triggered even if the OUI address does not match.

On a port operating in either macAddressElseUserLoginSecure mode or macAddressElseUserLoginSecureExt mode, Intrusion Protection is triggered only after both MAC-based authentication and 802.1x authentication on the same packet fail.

### Table 120 Description of port security modes

<table>
<thead>
<tr>
<th>Security mode</th>
<th>Description</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>macAddressElseUserLoginSecure</td>
<td>In this mode, a port first performs MAC authentication when a user attempts access. If that authentication fails, the port then performs 802.1x authentication. In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users.</td>
<td></td>
</tr>
<tr>
<td>macAddressElseUserLoginSecureExt</td>
<td>This mode is similar to the macAddressElseUserLoginSecure mode, except that there can be more than one 802.1x-authenticated user on the port.</td>
<td></td>
</tr>
<tr>
<td>macAddressAndUserLoginSecure</td>
<td>In this mode, a port first performs MAC authentication when a user attempts access. If that authentication is successful, the port then performs 802.1x authentication. This user must pass both authentication methods to gain network access. In this mode, only one user can access the network.</td>
<td></td>
</tr>
<tr>
<td>macAddressAndUserLoginSecureExt</td>
<td>This mode is similar to the macAddressAndUserLoginSecure mode, except that there can be more than one user can access the network.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 121 Port security configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling Port Security”</td>
<td>Required</td>
</tr>
<tr>
<td>“Setting the Maximum Number of MAC Addresses Allowed on a Port”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting the Port Security Mode”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring Port Security Features”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the NTK feature”</td>
<td></td>
</tr>
<tr>
<td>“Configuring intrusion protection”</td>
<td></td>
</tr>
<tr>
<td>“Configuring the Trap feature”</td>
<td></td>
</tr>
<tr>
<td>“Ignoring the Authorization Information from the RADIUS Server”</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Enabling Port Security

Configuration Prerequisites
Before enabling port security, you need to disable 802.1x and MAC authentication globally.

Configuration Procedure

<table>
<thead>
<tr>
<th>Table 121 Port security configuration tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
</tr>
<tr>
<td>&quot;Configuring Security MAC Addresses&quot;</td>
</tr>
</tbody>
</table>

Enabling Port Security

CAUTION: Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below):
- 802.1x (disabled), port access control method (macbased), and port access control mode (auto)
- MAC authentication (disabled)

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

<table>
<thead>
<tr>
<th>Table 122 Enable port security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Enable port security</td>
</tr>
</tbody>
</table>

CAUTION: Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below):

- 802.1x (disabled), port access control method (macbased), and port access control mode (auto)
- MAC authentication (disabled)

Setting the Maximum Number of MAC Addresses Allowed on a Port

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

By setting the maximum number of 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 Security MAC addresses that can be added with port security

This configuration is different from that of the maximum number of MAC addresses that can be leaned by a port in MAC address management.
Table 123 Set the maximum number of MAC addresses allowed on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of</td>
<td>port-security max-mac-count</td>
<td>Required</td>
</tr>
<tr>
<td>MAC addresses allowed on the port</td>
<td>count-value</td>
<td>Not limited by default</td>
</tr>
</tbody>
</table>

Table 124 Set the port security mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Set the OUI value for user       | port-security oui OUI-value index          | Optional, In userLoginWithOUI mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value.
| authentication                   | index-value                                |                                                                         |
| Enter Ethernet port view         | interface interface-type interface-number  | -                                                                        |
| Set the port security mode       | port-security port-mode { autolearn | mac-and-userlogin-secure | mac-and-userlogin-secure-ext | 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, By default, a port operates in noRestriction mode. In this mode, access to the port is not restricted. You can set a port security mode as needed. |

- Before setting the port security mode to autolearn, you need to set the maximum number of MAC addresses allowed on the port with the port-security max-mac-count command.
- When the port operates in the autolearn mode, you cannot change the maximum number of MAC addresses allowed on the port.
- After you set the port security mode to autolearn, you cannot configure any static or blackhole MAC addresses on the port.
- If the port is in a security mode other than noRestriction, before you can change the port security mode, you need to restore the port security mode to noRestriction with the undo port-security port-mode command.
- Fabric devices do not support autolearn port security mode.

If the port-security port-mode command has been executed on a port, none of the following can be configured on the same port:

- Maximum number of MAC addresses that the port can learn
- Reflector port for port mirroring
Fabric port

- Link aggregation

### Configuring Port Security Features

#### Configuring the NTK feature

<table>
<thead>
<tr>
<th>Table 125</th>
<th>Configure the NTK feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the NTK feature</td>
<td>port-security ntk-mode { ntkonly</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Configuring intrusion protection

<table>
<thead>
<tr>
<th>Table 126</th>
<th>Configure the intrusion protection feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Set the corresponding action to be taken by the switch when intrusion protection is triggered</td>
<td>port-security intrusion-mode { disableport</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
</tr>
<tr>
<td>Set the timer during which the port remains disabled</td>
<td>port-security timer disableport timer</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The `port-security timer disableport` command is used in conjunction with the `port-security intrusion-mode disableport-temporarily` command to set the length of time during which the port remains disabled.

**Caution:** If you configure the NTK feature and execute the `port-security intrusion-mode blockmac` command on the same port, the switch will be unable to disable the packets whose destination MAC address is illegal from being sent out that port; that is, the NTK feature configured will not take effect on the packets whose destination MAC address is illegal.

### Configuring the Trap feature

<table>
<thead>
<tr>
<th>Table 127</th>
<th>Configure port security trapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable sending traps for the specified type of event</td>
<td>port-security trap { addresslearned</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ignoring the Authorization Information from the RADIUS Server

After an 802.1x user or MAC-authenticated user passes Remote Authentication Dial-In User Service (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.

Table 128 Configure a port to ignore the authorization information from the RADIUS server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-number</td>
<td></td>
</tr>
<tr>
<td>Ignore the authorization</td>
<td>port-security authorization</td>
<td>Required</td>
</tr>
<tr>
<td>information from the RADIUS</td>
<td>ignore</td>
<td>By default, a port uses the</td>
</tr>
<tr>
<td>server</td>
<td></td>
<td>authorization information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>from the RADIUS server.</td>
</tr>
</tbody>
</table>

Configuring Security MAC Addresses

Security MAC addresses are special MAC addresses that never age out. One security MAC address can be added to only one port in the same VLAN so that you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security or manually configured.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses;
- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.

The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the switch reboots.

Configuration prerequisites

- Port security is enabled.
- The maximum number of security MAC addresses allowed on the port is set.
- The security mode of the port is set to **autolearn**.

Configuration procedure

Table 129 Configure a security MAC address

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
</tbody>
</table>
Displaying and Maintaining Port Security Configuration

After completing the above configuration, you can use the `display` command in any view to display port security information and verify your configuration.

### Table 129 Configure a security MAC address

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a security MAC address</td>
<td><code>mac-address security mac-address interface interface-type interface-number vlan vlan-id</code></td>
<td>Either is required. By default, no security MAC address is configured.</td>
</tr>
<tr>
<td>In Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mac-address security mac-address vlan vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>

### Displaying and Maintaining Port Security Configuration

Implement access user restrictions through the following configuration on Ethernet 1/0/1 of the switch.

- Allow a maximum of 80 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as security MAC addresses.
- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
- After the number of security MAC addresses reaches 80, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port will be disabled and stay silent for 30 seconds.

### Table 130 Display port security configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about port security configuration</td>
<td><code>display port-security [interface interface-list ]</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display information about security MAC address configuration</td>
<td><code>display mac-address security [interface interface-type interface-number ] [ vlan vlan-id ] [ count ]</code></td>
<td></td>
</tr>
</tbody>
</table>
Network diagram

Figure 56  Network diagram for port security configuration

[Network diagram]

Configuration procedure

# Enter system view.
<5500> system-view

# Enable port security.
[5500] port-security enable

# Enter Ethernet1/0/1 port view.
[5500] interface Ethernet 1/0/1

# Set the maximum number of MAC addresses allowed on the port to 80.
[5500-Ethernet1/0/1] port-security max-mac-count 80

# Set the port security mode to autolearn.
[5500-Ethernet1/0/1] port-security port-mode autolearn

# Add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
[5500-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1

# Configure the port to be silent for 30 seconds after intrusion protection is triggered.
[5500-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily
[5500-Ethernet1/0/1] quit
[5500] port-security timer disableport 30
Port Binding Configuration

Port Binding Overview

Introduction

Port binding enables the network administrator to bind the MAC address and IP address of a user to a specific port. After the binding, the switch forwards only the packets received on the port whose MAC address and IP address are identical with the bound MAC address and IP address. This improves network security and enhances security monitoring.

Configuring Port Binding

Table 131 Configure port binding

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Bind the MAC address and IP address of a user to a specific port</td>
<td>am user-bind mac-addr mac-address ip-addr ip-address interface interface-type interface-number</td>
<td>Either is required. By default, no user MAC address or IP address is bound to a port.</td>
</tr>
</tbody>
</table>

Table 132 Display port binding configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display port binding information</td>
<td>display am user-bind [ interface interface-type interface-number</td>
<td>You can execute the display command in any view.</td>
</tr>
</tbody>
</table>
Network requirements

It is required to bind the MAC and IP addresses of Host A to Ethernet 1/0/1 on Switch A, so as to prevent malicious users from using the IP address they steal from Host A to access the network.

Network diagram

Figure 57  Network diagram for port binding configuration

Configuration procedure

Configure Switch A as follows:

# Enter system view.

<5500> system-view

# Enter Ethernet 1/0/1 port view.

[5500] interface Ethernet 1/0/1

# Bind the MAC address and the IP address of Host A to Ethernet 1/0/1.

[5500-Ethernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
You may encounter unidirectional links in a network. When a unidirectional link occurs, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional links can cause problems such as loops in a Spanning Tree Protocol (STP) enabled network.

Unidirectional links can be caused by

- Fiber cross-connection, as shown in Figure 58.
- Fibers that are not connected or disconnected, as shown in Figure 59, the hollow lines in which refer to fibers that are not connected or disconnected.

Device link detection protocol (DLDP) can detect the link status of an optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it enables the related port automatically or prompts you to disable it manually according to the configurations, to avoid network problems.

**Figure 58** Fiber cross-connection
DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocols to monitor the link status of a device.
- The auto-negotiation mechanism at the physical layer detects physical signals and faults. DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- Even if both ends of links can work normally at the physical layer, DLDP can detect whether these links are connected correctly and whether packets can be exchanged normally at both ends. However, the auto-negotiation mechanism cannot implement this detection.
- In order for DLDP to detect fiber disconnection in one direction, you need to configure the port to work in mandatory full duplex mode at a mandatory rate.
- When the port determines the duplex mode and speed through auto-negotiation, even if DLDP is enabled, it does not take effect when the fiber in one direction is disconnected. In this case, the port is considered down.

**DLDP Fundamentals**

**Implementing DLDP**

DLDP detects link status by exchanging the packet types described in Table 133.

**Table 133** DLDP packet types

<table>
<thead>
<tr>
<th>DLDP packet type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement</td>
<td>Notifies the neighbor devices that the local device exists. An advertisement packet carries only the local port information, and does not require a response from the peer.</td>
</tr>
<tr>
<td>RSY-Advertisement packets (referred to as RSY packets hereafter)</td>
<td>Advertisement packet with the RSY flag set to 1. RSY advertisement packets request that the neighbor information is synchronized when that information is not locally available or when the information is outdated</td>
</tr>
<tr>
<td>Flush-Advertisement packets (referred to as flush packets hereafter)</td>
<td>Advertisement packet with the flush flag set to 1. A flush packet carries only the local port information (rather than the neighbor information) and is used to trigger neighbors to remove the information about the local device.</td>
</tr>
</tbody>
</table>
Overview

Probe packets are used to probe the existence of a neighbor. Echo packets are required from the corresponding neighbor. Probe packets carry the local port information. Neighbor information is optional for probe packets. A probe packet carrying neighbor information probes the specified neighbors; A probe packet carrying no neighbor information probes all the neighbors.

Echo packets are required to respond to probe packets. An echo packet carries the information about the response port and the neighbor information it maintains. Upon receiving an echo packet, a port checks whether the neighbor information carried in the echo packet is consistent with that of itself. If yes, the link between the local port and the neighbor is regarded as bidirectional.

Disable packets are used to notify the peer end that the local end is in the disable state. Disable packets carry only the local port information and not the neighbor information. When a port detects a unidirectional link and enters the disable state, the port sends disable packets to the neighbor. A port enters the disable state upon receiving a disable packet.

Linkdown packets are used to notify unidirectional link emergencies (a unidirectional link emergency occurs when the local port is down and the peer port is up). Linkdown packets carry only the local port information rather than the neighbor information. When a unidirectional link emergency occurs, DLDP sends linkdown packets immediately to inform the peer of the link abnormality. Without linkdown packets, the peer can detect the link abnormality only after a period when the corresponding neighbor information maintained on the neighbor device times out, which is three times the advertisement interval.

Upon receiving a linkdown packet, if the peer end operates in enhanced mode, enters the disable state, and sets the receiving port to the DLDP down state (auto shutdown mode) or issues an alarm to the user (manual shutdown mode).

Recover probe packets are used to detect whether a link recovers to implement the port auto-recovery mechanism. Recover probe packets carry only the local port information rather than the neighbor information. They request recover echo packets as the response. A port in the DLDP down state sends a recover probe packet every two seconds.

Recover echo packets respond to recover probe packets in the port auto-recovery mechanism. A link is considered to restore to the bidirectional state if a port on one end sends a recover probe packet, receives a recover echo packet, and the neighbor information contained in the recover echo packet is consistent with that of the local port.

Table 133  DLDP packet types

<table>
<thead>
<tr>
<th>DLDP packet type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe</td>
<td>Probe packets are used to probe the existence of a neighbor. Echo packets are required from the corresponding neighbor. Probe packets carry the local port information. Neighbor information is optional for probe packets. A probe packet carrying neighbor information probes the specified neighbors; A probe packet carrying no neighbor information probes all the neighbors.</td>
</tr>
<tr>
<td>Echo</td>
<td>Response to probe packets. An echo packet carries the information about the response port and the neighbor information it maintains. Upon receiving an echo packet, a port checks whether the neighbor information carried in the echo packet is consistent with that of itself. If yes, the link between the local port and the neighbor is regarded as bidirectional.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disable packets are used to notify the peer end that the local end is in the disable state. Disable packets carry only the local port information and not the neighbor information. When a port detects a unidirectional link and enters the disable state, the port sends disable packets to the neighbor. A port enters the disable state upon receiving a disable packet.</td>
</tr>
<tr>
<td>LinkDown</td>
<td>Linkdown packets are used to notify unidirectional link emergencies (a unidirectional link emergency occurs when the local port is down and the peer port is up). Linkdown packets carry only the local port information rather than the neighbor information. For the peer end, as Rx signals can still be received on the physical layer, the port is still considered to be normal. Such a situation is known as unidirectional link emergency. When a unidirectional link emergency occurs, DLDP sends linkdown packets immediately to inform the peer of the link abnormality. Without linkdown packets, the peer can detect the link abnormality only after a period when the corresponding neighbor information maintained on the neighbor device times out, which is three times the advertisement interval. Upon receiving a linkdown packet, if the peer end operates in enhanced mode, enters the disable state, and sets the receiving port to the DLDP down state (auto shutdown mode) or issues an alarm to the user (manual shutdown mode).</td>
</tr>
<tr>
<td>Recover Probe</td>
<td>Recover probe packets are used to detect whether a link recovers to implement the port auto-recovery mechanism. Recover probe packets carry only the local port information rather than the neighbor information. They request recover echo packets as the response. A port in the DLDP down state sends a recover probe packet every two seconds.</td>
</tr>
<tr>
<td>Recover Echo</td>
<td>Recover echo packets respond to recover probe packets in the port auto-recovery mechanism. A link is considered to restore to the bidirectional state if a port on one end sends a recover probe packet, receives a recover echo packet, and the neighbor information contained in the recover echo packet is consistent with that of the local port.</td>
</tr>
</tbody>
</table>
If the DLDP-enabled link is up, DLDP sends DLDP packets to the peer device, and analyzes/processes the DLDP packets received from the peer device. DLDP packets sent in different DLDP states are described in Table 134.

<table>
<thead>
<tr>
<th>DLDP state</th>
<th>Type of the DLDP packets sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Advertisement packets, with the RSY flag set or not set.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>Advertisement packets</td>
</tr>
<tr>
<td>Probe</td>
<td>Probe packets</td>
</tr>
</tbody>
</table>

The DLDP packet received is processed as follows:

- In authentication mode, the DLDP packet is authenticated and is then dropped if it fails the authentication.
- The packet is further processed, as described in Table 135.

Table 135 The procedure to process a received DLDP packet

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Processing procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement packet</td>
<td>Extracts neighbor information If the corresponding neighbor entry does not exist on the local device, DLDP creates the neighbor entry, triggers the entry aging timer, and switches to the probe state. If the corresponding neighbor entry already exists on the local device, DLDP resets the aging timer of the entry.</td>
</tr>
<tr>
<td>Flush packet</td>
<td>Removes the neighbor entry from the local device</td>
</tr>
<tr>
<td>Probe packet</td>
<td>Sends echo packets containing both neighbor and its own information to the peer      Create the neighbor entry if it does not exist on the local device. Resets the aging timer of the entry if the neighbor entry already exists on the local device.</td>
</tr>
<tr>
<td>Echo packet</td>
<td>Checks to see if the local device is in the probe state No Drops the echo packet    Checks to see if the neighbor information contained in the packet is the same as that on the local device No If all neighbors are in the bidirectional link state, DLDP switches from the probe state to the advertisement state, and sets the echo waiting timer to 0 Yes</td>
</tr>
</tbody>
</table>
If no echo packet is received from the neighbor, DLDP performs steps in Table 136.

**Table 136** Processing procedure when no echo packet is received from the neighbor

<table>
<thead>
<tr>
<th>No echo packet received from the neighbor</th>
<th>Processing procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>In normal mode, no echo packet is</td>
<td>DLDP switches to the disable state, outputs log and tracking information, and sends</td>
</tr>
<tr>
<td>received when the echo waiting timer</td>
<td>flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local</td>
</tr>
<tr>
<td>expires.</td>
<td>port automatically or prompts you to disable the port manually. DLDP sends RSY messages</td>
</tr>
<tr>
<td>In enhanced mode, no echo packet is</td>
<td>and removes the corresponding neighbor entries.</td>
</tr>
<tr>
<td>received when the enhanced timer expires</td>
<td></td>
</tr>
</tbody>
</table>

**IDLDp status**

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

**Table 137** DLDP status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Initial status before DLDP is enabled.</td>
</tr>
<tr>
<td>Inactive</td>
<td>DLDP is enabled but the corresponding link is down.</td>
</tr>
<tr>
<td>Active</td>
<td>DLDP is enabled, and the link is up or a neighbor entry is cleared.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>All neighbors communicate normally in both directions, or DLDP remains in active state for more than five seconds and enters this status. It is a stable state where no unidirectional link is found</td>
</tr>
<tr>
<td>Probe</td>
<td>DHCP sends packets to check whether the link is a unidirectional. It enables the probe sending timer and an echo waiting timer for each target neighbor.</td>
</tr>
<tr>
<td>Disable</td>
<td>DLDP detects a unidirectional link, or finds (in enhanced mode) that a neighbor disappears. In this case, DLDP sends and receives only recover probe packets and recover echo packets.</td>
</tr>
<tr>
<td>DelayDown</td>
<td>When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. After the DelayDown timer expires, the DLDP neighbor information is removed.</td>
</tr>
</tbody>
</table>

**DLDP Timers**

**Table 138** DLDP timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement sending timer</td>
<td>Interval between sending advertisement packets, which can be configured on a command line interface. By default, the timer length is 5 seconds.</td>
</tr>
<tr>
<td>Probe sending timer</td>
<td>The interval is 0.5 seconds. In the probe state, DLDP sends two probe packets in a second.</td>
</tr>
</tbody>
</table>
Table 138  DLDP timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
</tr>
</thead>
</table>
| Echo waiting timer | It is enabled when DLDP enters the probe state. The echo waiting timer length is 10 seconds.  
If no echo packet is received from the neighbor when the Echo waiting timer expires, the state of the local end is set to unidirectional link (one-way audio) and the state machine turns into the disable state. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. At the same time, DLDP deletes the neighbor entry. |
| Entry aging timer | When a new neighbor joins, a neighbor entry is created and the corresponding entry aging timer is enabled.  
When an advertisement packet is received from a neighbor, the neighbor entry is updated and the corresponding entry aging timer is updated.  
In the normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with an RSY tag, and deletes the neighbor entry.  
In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer.  
The entry aging timer length is three times the advertisement timer length. |
| Enhanced timer    | In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The enhanced timer length is 10 seconds.  
The enhanced timer then sends one probe packet every second and eight packets successively to the neighbor.  
If no echo packet is received from the neighbor when the enhanced timer expires, the state of the local end is set to unidirectional communication state and the state machine turns into the disable state. DLDP outputs log and tracking information and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. Meanwhile, DLDP deletes the neighbor entry. |
| DelayDown timer   | When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first.  
When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. The DelayDown timer is configurable and ranges from 1 to 5 seconds.  
A device in the delaydown state only responds to port up messages.  
A device in the delaydown state resumes its original DLDP state if it receives a port up message before the delaydown timer expires. Otherwise, it removes the DLDP neighbor information and changes to the inactive state. |
DLDP Operating Mode

DLDP can operate in two modes, normal and enhanced as described in Table 139.

<table>
<thead>
<tr>
<th>DLDP operating mode</th>
<th>DLDP detects whether neighbors exist or not when neighbor tables are aging</th>
<th>The entry aging timer is enabled or not during neighbor entry aging</th>
<th>The enhanced timer is enabled or not when the entry aging timer expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal mode</td>
<td>No</td>
<td>Yes (The neighbor entry ages out after the entry aging timer expires)</td>
<td>No</td>
</tr>
<tr>
<td>Enhanced mode</td>
<td>Yes</td>
<td>Yes (The enhanced timer is enabled after the entry aging timer expires)</td>
<td>Yes (When the enhanced timer expires, the state of the local end is set to unidirectional link, and the neighbor entry is aged out.)</td>
</tr>
</tbody>
</table>

DLDP Neighbor State

A DLDP neighbor can be in one of these two states: two way and unknown. You can check the state of a DLDP neighbor by using the `display dldp` command.

<table>
<thead>
<tr>
<th>DLDP neighbor state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two way</td>
<td>The link to the neighbor operates properly.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The device is detecting the neighbor and the neighbor state is unknown.</td>
</tr>
</tbody>
</table>

Link Auto-recovery Mechanism

If the shutdown mode of a port is set to auto shutdown, the port is set to the DLDP down state when DLDP detects the link connecting to the port is a unidirectional link. A port in DLDP down state does not forward service packets or receive/send protocol packets except DLDPDUs.

A port in the DLDP down state recovers when the corresponding link recovers. A port in the DLDP down state sends recover probe packets periodically. On receiving a correct recover echo packet (which means that the unidirectional link is restored to a bidirectional link), it is brought up by DLDP. The detailed process is as follows.

1. A port in the DLDP down state sends a recover probe packet every 2 seconds. Recover probe packets carry only the local port information.
2. Upon receiving a recover probe packet, the peer end responds with a recover echo packet.
3. Upon receiving a recover echo packet, the local end checks to see if the neighbor information carried in the recover echo packet is consistent with that of the local port. If yes, the link between the local port and the neighbor is considered to be recovered to bidirectional, the port changes from the disable state to the active state, and neighboring relationship is reestablished between the local port and the neighbor.
Only ports in the DLDP down state can send and process recover probe packets and recover echo packets. The auto-recovery mechanism does apply to ports that are shut down manually.

**DLDLP Configuration**

**Table 141** Perform basic DLDP configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable DLDP globally</td>
<td>dldp enable</td>
<td>Required.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>By default, DLDP is disabled.</td>
</tr>
<tr>
<td>Enable DLDP on a port</td>
<td>dldp enable</td>
<td></td>
</tr>
<tr>
<td>Set the authentication mode and password</td>
<td>dldp authentication-mode { none</td>
<td>simple simple-password</td>
</tr>
<tr>
<td>Set the interval of sending DLDP packets</td>
<td>dldp interval timer-value</td>
<td>By default, the interval is 5 seconds.</td>
</tr>
<tr>
<td>Set the delaydown timer</td>
<td>dldp delaydown-timer delaydown-time</td>
<td>Optional.</td>
</tr>
<tr>
<td>Set the DLDP handling mode when an unidirectional link is detected</td>
<td>dldp unidirectional-shutdown { auto</td>
<td>manual }</td>
</tr>
<tr>
<td>Set the DLDP operating mode</td>
<td>dldp work-mode { enhance</td>
<td>normal }</td>
</tr>
</tbody>
</table>

Note the following when performing basic DLDP configuration.

- DLDP works only when the link is up.
To ensure unidirectional links can be detected, make sure DLDP is enabled on both sides; and the interval for sending advertisement packets, authentication mode, and password are the same on both sides.

- The interval for sending advertisement packets ranges from 1 to 100 seconds and defaults to 5 seconds. You can adjust this setting as needed to enable DLDP to respond in time to link failures. If the interval is too long, STP loops may occur before unidirectional links are terminated; if the interval is too short, network traffic may increase in vain and available bandwidth decreases. Normally, the interval is shorter than one-third of the STP convergence time, which is generally 30 seconds.

- DLDP does not process any LACP event, and treats each link in the aggregation group as independent.

- When connecting two DLDP-enabled devices, make sure the software running on them is of the same version. Otherwise, DLDP may operate improperly.

- When you use the `dldp enable/dldp disable` command in system view to enable/disable DLDP on all optical ports of the switch, the configuration takes effect on the existing optical ports, instead of those added subsequently.

- Make sure the authentication mode and password configured on both sides are the same for DLDP to operate properly.

- When DLDP works in enhanced mode, the system can identify two types of unidirectional links: one is caused by fiber cross-connection and the other is caused by one fiber being not connected or being disconnected.

- When DLDP works in normal mode, the system can identify unidirectional links caused by fiber cross-connection.

- When the device is busy with services and the CPU utilization is high, DLDP may issue mistaken reports. You are recommended to configure the operating mode of DLDP as manual after unidirectional links are detected, so as to reduce the influence of mistaken reports.

### Resetting DLDP State

You can reset the DLDP state for the ports shut down by DLDP due to unidirectional links to enable DLDP detection again.

> This function is only applicable to ports that are in DLDP down state.

<table>
<thead>
<tr>
<th>Table 142</th>
<th>Reset DLDP state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Reset DLDP state for all the ports shut down by DLDP</td>
<td><code>system-view</code>&lt;br&gt;<code>dldp reset</code></td>
</tr>
<tr>
<td>Reset the DLDP state for a port shut down by DLDP</td>
<td><code>interface interface-type interface-number</code>&lt;br&gt;<code>dldp reset</code></td>
</tr>
</tbody>
</table>

### Displaying and Maintaining DLDP

<table>
<thead>
<tr>
<th>Table 143</th>
<th>Display and maintain DLDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Display the DLDP configuration of a unit or a port</td>
<td>`display dldp { unit-id</td>
</tr>
</tbody>
</table>
**DLDP Configuration Example**

**Network requirements**

As shown in Figure 60,

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP. All the ports involved operate in mandatory full duplex mode, with their rates all being 1,000 Mbps.
- Suppose the fibers between Switch A and Switch B are cross-connected. DLDP disconnects the unidirectional links after detecting them.
- After the fibers are connected correctly, the ports shut down by DLDP are restored.

**Network diagram**

**Figure 60** Network diagram for DLDP configuration

![Network diagram for DLDP configuration](image)

**Configuration procedure**

1. Configure Switch A

   # Configure the ports to work in mandatory full duplex mode at a rate of 1,000 Mbps.

   ```
   <SwitchA> system-view
   [SwitchA] interface gigabitethernet 2/1/3
   [SwitchA-GigabitEthernet2/1/3] duplex full
   [SwitchA-GigabitEthernet2/1/3] speed 1000
   [SwitchA-GigabitEthernet2/1/3] quit
   [SwitchA] interface gigabitethernet 2/1/4
   [SwitchA-GigabitEthernet2/1/4] duplex full
   [SwitchA-GigabitEthernet2/1/4] speed 1000
   [SwitchA-GigabitEthernet2/1/4] quit
   # Enable DLDP globally.
   [SwitchA] dldp enable
   # Set the interval for sending DLDP packets to 15 seconds.
   [SwitchA] dldp interval 15
   # Configure DLDP to work in enhanced mode.
   [SwitchA] dldp work-mode enhance
   # Set the DLDP handling mode for unidirectional links to auto.
   [SwitchA] dldp unidirectional-shutdown auto
   # Display the DLDP state.
   [5500A] display dldp 1
   ```
When two switches are connected through fibers in a crossed way, two or three ports may be in the disable state, and the rest in the inactive state.

When a fiber is connected to a device correctly on one end with the other end connected to no device:

- If the device operates in the normal DLDP mode, the end that receives optical signals is in the advertisement state; the other end is in the inactive state.
- If the device operates in the enhance DLDP mode, the end that receives optical signals is in the disable state; the other end is in the inactive state.

# Restore the ports shut down by DLDP.

[5500A] dldp reset

2 Configure Switch B

The configuration of Switch B is the same to that of Switch A and is thus omitted.
MAC ADDRESS TABLE MANAGEMENT

By default, no Switch 5500 Ethernet is configured with a MAC address. Therefore, when the switch sends Layer 2 protocol packets, for example, STP, it uses the MAC address predefined in the protocol as the source address to send the packets, as it cannot obtain the MAC address of the sending port. In real networking, as multiple devices use the same source MAC address to send Layer 2 protocol packets, different ports on a device may learn the same MAC address, thus affecting the maintenance of the MAC address table.

To avoid the above mentioned problem, the Switch 5500 allows you to configure MAC addresses of the local device’s Ethernet ports by specifying only the start one, that is, the MAC address of Ethernet 1/0/1. Once you specify the MAC address of the port with the smallest port number, each of the following ports uses the MAC address of the preceding port plus 1 as its own MAC address.

For example, if you configure the MAC address of Ethernet 1/0/1 as 000f-e200-0001, then port Ethernet 1/0/2 will automatically define its MAC address as 000f-e200-0002, and so on.

Follow these steps in Table 144 to configure the start MAC address of Ethernet ports (this does not apply to the Switch 5500G).

<table>
<thead>
<tr>
<th>Table 144 Configuring the start MAC address of Ethernet ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Configure the start MAC address of Ethernet ports</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The start MAC address you set must be a valid unicast address, and cannot be a broadcast or multicast address, or an address of all 0s or all Fs.

After you configure a port’s MAC address, the switch uses the sending port’s MAC address as the source MAC address when sending the following Layer 2 protocol packets:

- LACP
- STP
- NDP/NTDP
- GVRP
- DLDP
The MAC address configuration does not affect the normal forwarding of service packets.

- This chapter describes how to manage of static, dynamic, and blackhole MAC address entries. For information about managing multicast MAC address entries, refer to “Multicast Protocols” on page 392.
- The configuration of enabling destination MAC address triggered update is added. For the detailed configuration, refer to Enabling Destination MAC Address Triggered Update.
- The configuration of setting the MAC address of an Ethernet port is added. For the detailed configuration, refer to Configuring the MAC Address of an Ethernet Port

### Introduction to the MAC Address Table

An Ethernet switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding egress port numbers on the local switch

When forwarding a packet, an Ethernet switch adopts one of the two forwarding methods based upon the MAC address table entries.

- Unicast forwarding: If the destination MAC address carried in the packet is included in a MAC address table entry, the switch forwards the packet through the forwarding egress port in the entry.
- Broadcast forwarding: If the destination MAC address carried in the packet is not included in the MAC address table, the switch broadcasts the packet to all ports except the one receiving the packet.

### Introduction to MAC Address Learning

MAC address table entries can be updated and maintained through the following two ways:

- Manual configuration
- MAC address learning

Generally, the majority of MAC address entries are created and maintained through MAC address learning. The following describes the MAC address learning process of a switch:

1. As shown in Figure 61, User A and User B are both in VLAN 1. When User A communicates with User B, the packet from User A needs to be transmitted to Ethernet 1/0/1. At this time, the switch records the source MAC address of the
packet, that is, the address **MAC-A** of User A to the MAC address table of the switch, forming an entry shown in Figure 62.

**Figure 61**  MAC address learning diagram (1)

![MAC address learning diagram (1)](image1)

**Figure 62**  MAC address table entry of the switch (1)

<table>
<thead>
<tr>
<th>MAC-address</th>
<th>Port</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-A</td>
<td>Ethernet1/0/1</td>
<td>1</td>
</tr>
</tbody>
</table>

2 After learning the MAC address of User A, the switch starts to forward the packet. Because there is no MAC address and port information of User B in the existing MAC address table, the switch forwards the packet to all ports except Ethernet 1/0/1 to ensure that User B can receive the packet.

**Figure 63**  MAC address learning diagram (2)

![MAC address learning diagram (2)](image2)

3 Because the switch broadcasts the packet, both User B and User C can receive the packet. However, User C is not the destination device of the packet, and therefore does not process the packet. Normally, User B will respond to User A, as shown in Figure 64. When the response packet from User B is sent to Ethernet 1/0/4, the
switch records the association between the MAC address of User B and the corresponding port to the MAC address table of the switch.

**Figure 64** MAC address learning diagram (3)

![MAC address learning diagram](image)

4 At this time, the MAC address table of the switch includes two forwarding entries shown in Figure 65. When forwarding the response packet, the switch unicasts the packet instead of broadcasting it to User A through Ethernet 1/0/1, because MAC-A is already in the MAC address table.

**Figure 65** MAC address table entries of the switch (2)

<table>
<thead>
<tr>
<th>MAC-address</th>
<th>Port</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-A</td>
<td>Ethernet1/0/1</td>
<td>1</td>
</tr>
<tr>
<td>MAC-B</td>
<td>Ethernet1/0/4</td>
<td>1</td>
</tr>
</tbody>
</table>

5 After this interaction, the switch directly unicasts the communication packets between User A and User B based on the corresponding MAC address table entries.

- Under some special circumstances, for example, User B is unreachable or User B receives the packet but does not respond to it, the switch cannot learn the MAC address of User B. Hence, the switch still broadcasts the packets destined for User B.
- The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

---

**Managing the MAC Address Table**

**MAC address table aging**

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch starts an aging timer for an entry when dynamically creating the entry. The switch removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time.
Aging timer only takes effect on dynamic MAC address entries.

Entries in a MAC address table
Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually and can not age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change.

- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.

- Blackhole MAC address entry: This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries.

Table 145 lists the different types of MAC address entries and their characteristics.

<table>
<thead>
<tr>
<th>MAC address entry</th>
<th>Configuration method</th>
<th>Aging time</th>
<th>Reserved or not at reboot (if the configuration is saved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static MAC address entry</td>
<td>Manually configured</td>
<td>Unavailable</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic MAC address entry</td>
<td>Manually configured or generated by MAC address learning mechanism</td>
<td>Available</td>
<td>No</td>
</tr>
<tr>
<td>Blackhole MAC address entry</td>
<td>Manually configured</td>
<td>Unavailable</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Configuring MAC Address Table Management

Table 146 Configure MAC address table management

<table>
<thead>
<tr>
<th>Related section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring a MAC Address Entry”</td>
<td>Required</td>
</tr>
<tr>
<td>“Setting the Aging Time of MAC Address Entries”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting the Maximum Number of MAC Addresses a Port Can Learn”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Enabling Destination MAC Address Triggered Update”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the MAC Address of an Ethernet Port”</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Configuring a MAC Address Entry

You can add, modify, or remove a MAC address entry, remove all MAC address entries concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

You can add a MAC address entry in either system view or Ethernet port view.

Adding a MAC address entry in system view

Table 147  Add a MAC address entry in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Add a MAC address entry</td>
<td>mac-address { static</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

⚠️ CAUTION:

- When you add a MAC address entry, the port specified by the interface argument must belong to the VLAN specified by the vlan argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the vlan argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Adding a MAC address entry in Ethernet port view

Table 148  Add a MAC address entry in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Add a MAC address entry</td>
<td>mac-address { static</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

⚠️ CAUTION:

- When you add a MAC address entry, the current port must belong to the VLAN specified by the vlan argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the vlan argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Setting the Aging Time of MAC Address Entries

Setting aging time properly helps effective utilization of MAC address aging. The aging time that is too long or too short affects the performance of the switch.

- If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.
Configuring MAC Address Table Management

Normally, you are recommended to use the default aging time, namely, 300 seconds. The `no-aging` keyword specifies that MAC address entries do not age out.

MAC address aging configuration applies to all ports, but only takes effect on dynamic MAC addresses that are learnt or configured to age.

Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. By searching the MAC address table, the switch directly forwards the packets destined for these MAC addresses through the hardware, improving the forwarding efficiency. A MAC address table too big in size may prolong the time for searching MAC address entries, thus decreasing the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, the administrator can control the number of the MAC address entries the MAC address table can dynamically maintain. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Table 149  Set aging time of MAC address entries

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Set the aging time of MAC address entries</td>
<td>`mac-address timer { aging age</td>
<td>no-aging }`</td>
</tr>
</tbody>
</table>

If you have configured the maximum number of MAC addresses that a port can learn, you cannot enable the MAC authentication and port security functions on the port. Or, if you have enabled the MAC authentication and port security functions on a port, you cannot configure the maximum number of MAC addresses that the port can learn.

Enabling Destination MAC Address Triggered Update

By default, a switch updates its MAC address entries according to only source MAC addresses of packets. However, this may cause the switch to perform unnecessary broadcasts in some applications. For example, when a port aggregation group is used in an IRF fabric for communications, MAC address entries of some ports in the aggregation group may not be updated in time, resulting in unnecessary broadcasts.
The destination MAC address triggered update function solves the above problem by allowing the switch to update its MAC address entries according to destination MAC addresses of packets too. This function improves the availability of the MAC address table.

Follow the steps in Table 151 to enable destination MAC address triggered update:

**Table 151  Enabling destination port MAC address-triggered update**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Enable destination MAC address triggered update | mac-address aging destination-hit enable | Required
|                       |                       | Disabled by default |

**Table 152  Configuring the MAC address of an Ethernet port**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Configure the start MAC address of Ethernet ports | port-mac start-mac-address | Required
|                                |                   | No start MAC address of Ethernet ports is configured by default. |

The start MAC address you set must be a valid unicast address, and cannot be a broadcast or multicast address, or an address of all 0s or all Fs.

After you configure a port’s MAC address, the switch uses the MAC address of the sending port as the source MAC address when sending the following Layer 2 protocol packets:

- LACP
- STP
- NDP/NTDP
- GVRP
- DLDP

Configuring the MAC address does not affect the normal forwarding of service packets.

**Displaying MAC Address Table Information**

To verify your configuration, you can display information about the MAC address table by executing the `display` command in any view.

**Table 153 Display MAC address table information**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the MAC address table</td>
<td><code>display mac-address</code></td>
<td>The <code>display</code> command can be executed in any view.</td>
</tr>
<tr>
<td>Display the aging time of the dynamic MAC address entries in the MAC address table</td>
<td><code>display mac-address aging-time</code></td>
<td></td>
</tr>
<tr>
<td>Display the configured start MAC address of Ethernet ports</td>
<td><code>display port-mac</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Example**

**Adding a Static MAC Address Entry Manually**

**Network requirements**

The server connects to the switch through Ethernet 1/0/2. To prevent the switch from broadcasting packets destined for the server, it is required to add the MAC address of the server to the MAC address table of the switch, which then forwards packets destined for the server through Ethernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port Ethernet 1/0/2 belongs to VLAN 1.

**Configuration procedure**

# Enter system view.

```
<5500> system-view
[5500]
```

# Add a MAC address, with the VLAN, ports, and states specified.

```
[5500] mac-address static 000f-e20f-dc71 interface Ethernet 1/0/2 vlan 1
```

# Display information about the current MAC address table.

```
[5500] display mac-address interface Ethernet 1/0/2
MAC ADDR     VLAN ID STATE     PORT INDEX  AGING TIME(s)
000f-e20f-dc71 1  Config static Ethernet1/0/2  NOAGED
000f-e20f-a7d6 1  Learned     Ethernet1/0/2  AGING
000f-e20f-b1fb 1  Learned     Ethernet1/0/2  AGING
000f-e20f-f116 1  Learned     Ethernet1/0/2  AGING
--- 4 mac address(es) found on port Ethernet1/0/2 ---
```
The Auto Detect function uses ICMP request/reply packets to test network connectivity regularly.

The detected object of the Auto Detect function is a detected group, which is a set of IP addresses. To check the reachability to a detected group, a switch enabled with Auto Detect sends ICMP requests to the group and waits for the ICMP replies from the group based on the user-defined policy (which includes the number of ICMP requests and the timeout waiting for a reply). Then according to the check result, the switch determines whether to make the applications using the detected group take effect.

Currently, the following features are used in conjunction with Auto Detect:

- Static route
- Virtual Router Redundancy Protocol (VRRP)
- Interface backup

A detected group can be used by multiple applications simultaneously.

For details about static routing, refer to the chapter entitled “IP Routing Protocol Overview” on page 277.

For details about VRRP, refer to “VRRP Configuration” on page 553.

### Table 154 Auto Detect configuration tasks

<table>
<thead>
<tr>
<th>Configuration tasks</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Auto Detect Basic Configuration”</td>
<td>Required</td>
</tr>
<tr>
<td>“Auto Detect Implementation in Static Routing”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Auto Detect Implementation in VRRP”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Auto Detect Implementation in VLAN Interface Backup”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Table 155 Configure the auto detect function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a detected group and enter detected group view</td>
<td>detect-group group-number</td>
<td>Required</td>
</tr>
</tbody>
</table>
If the relationship between IP addresses of a detected group is and, any unreachable IP address in the group makes the detected group unreachable and the remaining IP addresses will not be detected. If the relationship is or, any reachable IP address makes the detected group reachable and the remaining IP addresses will not be detected.

### Auto Detect Implementation in Static Routing

You can bind a static route with a detected group. The Auto Detect function will then detect the reachability of the static route through the path specified in the detected group.

- The static route is valid if the detected group is reachable.
- The static route is invalid if the detected group is unreachable.

You need to create the detected group before performing the following operations.

### Table 155  Configure the auto detect function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an IP address to be detected to the detected group</td>
<td>detect-list list-number ip address ip-address [ nexthop ip-address ]</td>
<td>Required</td>
</tr>
<tr>
<td>Specify a relationship between detected IP addresses in the group</td>
<td>option [ and</td>
<td>or ]</td>
</tr>
<tr>
<td>Set an interval between detecting operations</td>
<td>timer loop interval</td>
<td>Optional, By default, the detecting interval is 15 seconds.</td>
</tr>
<tr>
<td>Set the number of ICMP requests during a detecting operation</td>
<td>retry retry-times</td>
<td>Optional, By default, the number is 2.</td>
</tr>
<tr>
<td>Set a timeout waiting for an ICMP reply</td>
<td>timer wait seconds</td>
<td>Optional, By default, the timeout is 2 seconds.</td>
</tr>
<tr>
<td>Display the detected group configuration</td>
<td>display detect-group [ group-number ]</td>
<td>Available in any view</td>
</tr>
</tbody>
</table>

### Table 156  Configure the auto detect function for a static route

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Bind a detected group to a static route</td>
<td>ip route-static ip-address { mask</td>
<td>mask-length } { interface-type interface-number</td>
</tr>
</tbody>
</table>
Auto Detect Implementation in VRRP

You can enable Auto Detect on the master switch in a VRRP group, use the Auto Detect function to detect the routes from the master switch to other networks, and use the detection results (reachable/unreachable) to control the priority of the master switch, so as to realize the automatic master-backup switchover:

- The master switch keeps as Master when the detected group is reachable.
- The priority of the master switch decreases and thus becomes a Backup when the detected group is unreachable.

You need to create the detected group and perform VRRP-related configurations before issuing the commands in Table 157.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable the auto detect function for VRRP</td>
<td>vrrp vrid virtual-router-id track detect-group group-number [ reduced value-reduced ]</td>
<td>Required</td>
</tr>
</tbody>
</table>

Auto Detect Implementation in VLAN Interface Backup

Using Auto Detect can help realize VLAN interfaces backup. When data can be transmitted through two VLAN interfaces on the switch to the same destination, configure one of the VLAN interface as the active interface and the other as the standby interface. The standby interface is enabled automatically when the active fails, so as to ensure the data transmission. In this case, the Auto Detect function is implemented as follows:

- In normal situations (that is, when the detected group is reachable), the standby VLAN interface is down and packets are transmitted through the active VLAN interface.
- When the link between the active VLAN interface and the destination faults (that is, the detected group is unreachable), the system enables the backup VLAN interface.
- When the link between the active VLAN interface and the destination recovers (that is, the detected group becomes reachable again), the system shuts down the standby VLAN interface again.

You need to create the detected group and perform configurations concerning VLAN interfaces before the following operations.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable the auto detect function to implement VLAN interface backup</td>
<td>standby detect-group group-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This operation is only needed on the secondary VLAN interface.</td>
</tr>
</tbody>
</table>
Auto Detect Configuration Example

Network requirements

- Create detected group 8 on Switch A; detect the reachability of the IP address 10.1.1.4, with 192.168.1.2 as the next hop, and the detecting number set to 1.
- On switch A, configure a static route to Switch C.
- Enable the static route when the detected group 8 is reachable.
- To ensure normal operation of the auto detect function, configure a static route to Switch A on Switch C.

Network diagram

Figure 66  Network diagram for implementing the auto detect function in static route

Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 66.

- Configure Switch A.

  # Enter system view.

  <SwitchA> system-view

  # Create detected group 8.

  [SwitchA] detect-group 8

  # Detect the reachability of 10.1.1.4/24, with 192.168.1.2/24 as the next hop, and the detecting number set to 1.

  [SwitchA-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
  [SwitchA-detect-group-8] quit

  # Enable the static route when the detected group is reachable. The static route is invalid when the detected group is unreachable.

  [SwitchA] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8

  Configure Switch C.

  # Enter system view.
  <SwitchC> system-view
# Configure a static route to Switch A.

[SwitchC] ip route-static 192.168.1.1 24 10.1.1.3

Network requirements
- Switch A and switch B form VRRP backup group 1, whose virtual IP address is 192.168.1.10.
- Packets sourced from Host A and destined for Host B is forwarded by Switch B under normal situations.
- When the connection between Switch A and Switch B fails, Switch B becomes the master in the VRRP group 1 automatically and the link from Switch B to Host B, the backup link, is enabled.

Network diagram

Figure 67 Network diagram for implementing the auto detect function in VRRP

Configuration procedure
Configure the IP addresses of all the interfaces as shown in Figure 67.
- Configure Switch B.

# Create detected group 9.

<SwitchA> system-view
[SwitchA] detect-group 9

# Specify to detect the reachability of the IP address 10.1.1.4/24, setting the detect number to 1.

[SwitchA-detect-group-9] detect-list 1 ip address 10.1.1.4
[SwitchA-detect-group-9] quit

# Enable VRRP on VLAN-interface 1 and assign a virtual IP address to the VRRP group.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10

# Set the VRRP group priority of switch A to 110, and specify to decrease the priority by 20 when the result of detected group 9 is unreachable.

[SwitchA-Vlan-interface1] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface1] vrrp vrid 1 track detect-group 9 reduced 20

Configure Switch B.

# Enable VRRP on VLAN-interface 1 and assign a virtual IP address to the VRRP group.

<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10

# Set the VRRP group priority of Switch B to 100.

[SwitchB-Vlan-interface1] vrrp vrid 1 priority 100

Configuration Example for Auto Detect Implementation in VLAN Interface Backup

Network requirements
- Make sure the routes between Switch A, Switch B, and Switch C, and between Switch A, Switch D, and Switch C are reachable.
- Create detected group 10 on Switch A to detect the connectivity between Switch B and Switch C.
- Configure VLAN-interface 1 to be the active interface, which is enabled when the detected group 10 is reachable.
- Configure VLAN-interface 2 to be the standby interface, which is enabled when the detected group 10 is unreachable.
Network diagram

Figure 68  Network diagram for VLAN interface backup

Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 68.

# Enter system view.

<SwitchA> system-view

# Create auto detected group 10.

[SwitchA] detect-group 10

# Add the IP address of 10.1.1.4 to detected group 10 to detect the reachability of the IP address, with the IP address of 192.168.1.2 as the next hop, and the detecting number set to 1.

[SwitchA-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[SwitchA-detect-group-10] quit

# Specify to enable VLAN-interface 2 when the result of detected group 10 is unreachable.

[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] standby detect-group 10

# Add the IP address of 10.1.1.4 to detected group 10 to detect the reachability of the IP address, with the IP address of 192.168.1.2 as the next hop, and the detecting number set to 1.
[5500-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[5500-detect-group-10] quit

# Specify to enable VLAN INTERFACE 2 when the result of detected group 10 is unreachable.

[5500] interface vlan-interface 2
[5500-Vlan-interface2] standby detect-group 10
MSTP CONFIGURATION

STP Overview

Functions of STP

Spanning tree protocol (STP) is a protocol conforming to IEEE 802.1d. It aims to eliminate loops on data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging packets with one another and eliminate the loops detected by blocking specific ports until the network is pruned into one with tree topology. As a network with tree topology is loop-free, it prevents packets in it from being duplicated and forwarded endlessly and prevents device performance degradation.

Currently, in addition to the protocol conforming to IEEE 802.1d, STP also refers to the protocols based on IEEE 802.1d, such as RSTP, and MSTP.

Protocol packets of STP

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

STP identifies the network topology by transmitting BPDUs between STP compliant network devices. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used to calculate spanning trees and maintain the spanning tree topology.
- Topology change notification (TCN) BPDUs, used to notify 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 has been introduced in STP.

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

Upon network convergence, the root bridge generates and sends out configuration BPDUs periodically. Other devices just forward the configuration BPDUs received. This mechanism ensures the topological stability.

2 Root port

On a non-root bridge device, the root port is the port with the lowest path cost to the root bridge. The root port is used for communicating with the root bridge. A
non-root-bridge device has one and only one root port. The root bridge has no root port.

3 Designated bridge and designated port

Refer to Table 159 for the description of designated bridge and designated port.

Table 159 Designated bridge and designated port

<table>
<thead>
<tr>
<th>Classification</th>
<th>Designated bridge</th>
<th>Designated port</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a device</td>
<td>A designated bridge is a device that is directly connected to a switch and is</td>
<td>The port through which the designated bridge forwards BPDUs to this device</td>
</tr>
<tr>
<td></td>
<td>responsible for forwarding BPDUs to this switch.</td>
<td></td>
</tr>
<tr>
<td>For a LAN</td>
<td>A designated bridge is a device responsible for forwarding BPDUs to this LAN</td>
<td>The port through which the designated bridge forwards BPDUs to this LAN segment.</td>
</tr>
<tr>
<td></td>
<td>segment.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 69 shows designated bridges and designated ports. In the figure, 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 is the 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 is the port BP2 on Device B.

Figure 69 A schematic diagram of designated bridges and designated ports

All the ports on the root bridge are designated ports.

4 Path cost

Path cost is a value used for measuring link capacity. By comparing the path costs of different links, STP selects the most robust links and blocks the other links to prune the network into a tree.
How STP works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID, consisting of root bridge priority and MAC address.
- Root path cost, the cost of the shortest path to the root bridge.
- Designated bridge ID, designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port name.
- Message age: lifetime for the configuration BPDUs to be propagated within the network.
- Max age, lifetime for the configuration BPDUs to be kept in a switch.
- Hello time, configuration BPDU interval.
- Forward delay, forward delay of the port.

For the convenience of description, the description and examples below involve only four parts of a configuration BPDU:

- Root bridge ID (in the form of device priority)
- Root path cost
- Designated bridge ID (in the form of device priority)
- Designated port ID (in the form of port name)

1 Detailed calculation process of the STP algorithm

- Initial state
  
  Upon initialization of a device, each device 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.

- Selection of the optimum configuration BPDU
  
  Each device sends out its configuration BPDU and receives configuration BPDU from other devices.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Upon receiving a configuration BPDU on a port, the device performs the following processing:
|      | - If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. |
|      | - If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU. |
| 2    | The device compares the configuration BPDU of all the ports and chooses the optimum configuration BPDU. |
Principle for configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.

- If all the configuration BPDU have the same root bridge ID, they will be compared for their root path costs. If the root path cost in a configuration BPDU plus the path cost corresponding to this port is S, the configuration BPDU with the smallest S value has the highest priority.

- If all configuration BPDU have the same root path cost, the following configuration BPDU priority is compared sequentially: designated bridge IDs, designated port IDs, and then the IDs of the ports on which the configuration BPDU are received. The switch with a higher priority is elected as the root bridge.

Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own bridge ID. By exchanging configuration BPDUs, the devices compare one another's root bridge ID. The device with the smallest root bridge ID is elected as the root bridge.

Selection of the root port and designated ports

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

Table 161  Selection of the root port and designated ports

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A non-root-bridge device takes the port on which the optimum configuration BPDU was received as the root port.</td>
</tr>
<tr>
<td>2</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- The root bridge ID is replaced with that of the configuration BPDU of the root port.</td>
</tr>
<tr>
<td></td>
<td>- The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port.</td>
</tr>
<tr>
<td></td>
<td>- The designated bridge ID is replaced with the ID of this device.</td>
</tr>
<tr>
<td></td>
<td>- The designated port ID is replaced with the ID of this port.</td>
</tr>
<tr>
<td>3</td>
<td>The device compares the calculated configuration BPDU with the configuration BPDU on the port whose role is to be determined, and acts as follows based on the comparison result:</td>
</tr>
<tr>
<td></td>
<td>- If the calculated configuration BPDU is superior, this port will serve as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically.</td>
</tr>
<tr>
<td></td>
<td>- If the configuration BPDU on the port is superior, the device stops updating the configuration BPDUs of the port and blocks the port, so that the port only receives configuration BPDUs, but does not forward data or send configuration BPDUs.</td>
</tr>
</tbody>
</table>

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 only receive STP packets but do not forward user traffic.

Once the root bridge, the root port on each non-root bridge and designated ports have been successfully elected, the entire tree-shaped topology has been constructed.
The following is an example of how the STP algorithm works. The specific network diagram is shown in Figure 70. 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 70** Network diagram for STP algorithm

- **Initial state of each device**
  The following table shows the initial state of each device.

<table>
<thead>
<tr>
<th>Device</th>
<th>Port name</th>
<th>BPDU of port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device A</td>
<td>AP1</td>
<td>{0, 0, 0, AP1}</td>
</tr>
<tr>
<td></td>
<td>AP2</td>
<td>{0, 0, 0, AP2}</td>
</tr>
<tr>
<td>Device B</td>
<td>BP1</td>
<td>{1, 0, 1, BP1}</td>
</tr>
<tr>
<td></td>
<td>BP2</td>
<td>{1, 0, 1, BP2}</td>
</tr>
<tr>
<td>Device C</td>
<td>CP1</td>
<td>{2, 0, 2, CP1}</td>
</tr>
<tr>
<td></td>
<td>CP2</td>
<td>{2, 0, 2, CP2}</td>
</tr>
</tbody>
</table>

- **Comparison process and result on each device**
  The following table shows the comparison process and result on each device.
<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>BPDU of port after comparison</th>
</tr>
</thead>
</table>
| 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 configuration received message, and discards the received configuration BPDU.  
                  ■ 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 discards the received configuration BPDU.  
                  ■ Device A finds that both the root bridge and designated bridge in the configuration BPDU of all its ports are Device A 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}                          |
|            |                                                                                                                                      | 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.  
                  ■ 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 discards the received configuration BPDU.  
                  ■ 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.  
                  ■ 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}.  
                  ■ Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If 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. | BP1: {0, 0, 0, AP1}                          |
|            |                                                                                                                                      | BP2: {1, 0, 1, BP2}                          |
|            |                                                                                                                                      | Root port BP1: {0, 0, 0, AP1}                |
|            |                                                                                                                                      | Designated port BP2: {0, 5, 1, BP2}          |
After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in Figure 71.

Table 163  Comparison process and result on each device

<table>
<thead>
<tr>
<th>Device</th>
<th>Comparison process</th>
<th>BPDU of port after comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device C</td>
<td>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.</td>
<td>CP1: (0, 0, 0, AP2)</td>
</tr>
<tr>
<td></td>
<td>Port CP2 receives the configuration BPDU of port BP2 of Device B (1, 0, 1, BP2) before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port (2, 0, 2, CP2), and updates the configuration BPDU of CP2.</td>
<td>CP2: (1, 0, 1, BP2)</td>
</tr>
<tr>
<td></td>
<td>By comparison:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDU of which will not be changed.</td>
<td>Root port CP1: (0, 0, 0, AP2)</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
<td>Designated port CP2: (0, 10, 2, CP2)</td>
</tr>
<tr>
<td></td>
<td>■ Next, port CP2 receives the updated configuration BPDU of Device B (0, 5, 1, BP2). Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ At the same time, port CP1 receives configuration BPDU periodically from Device A. Device C does not launch an update process after comparison.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By comparison:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Because the root path cost of CP2 (9) (root path cost of the BPDU (5) + 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.</td>
<td>Blocked port CP2: (0, 0, 0, AP2)</td>
</tr>
<tr>
<td></td>
<td>■ 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 remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down.</td>
<td>Block port CP2: (0, 0, AP2)</td>
</tr>
</tbody>
</table>

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in Figure 71.
To facilitate description, the spanning tree calculation process in this example is simplified, while the actual process is more complicated.

2 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 interval of hello time.

- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.

- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately sends out its better 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 generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established 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 through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

3 STP timers

The following three time parameters are important for STP calculation:

- Forward delay, the period a device waits before state transition.

A link failure triggers a new round of spanning tree calculation and results in changes of the spanning tree. However, as new configuration BPDUs cannot be propagated throughout the network immediately, if the new root port and
designated port begin to forward data as soon as they are elected, loops may temporarily occur.

For this reason, the protocol uses a state transition mechanism. Namely, a newly elected root port and the designated ports must go through a period, which is twice the forward delay time, before they transit to the forwarding state. The period allows the new configuration BPDUs to be propagated throughout the entire network.

- Hello time, the interval for sending hello packets. Hello packets are used to check link state.

A switch sends hello packets to its neighboring devices at a regular interval (the hello time) to check whether the links are faulty.

- Max time, lifetime of the configuration BPDUs stored in a switch. A configuration BPDU that has expired is discarded by the switch.

MSTP Overview

**Background of MSTP**

Disadvantages 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 it is an edge port (an edge port refers to a port that 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 reach the final topology stability.

- In RSTP, the state of a root port can transit fast under the following conditions: the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.

- In RSTP, the state of a designated port can transit fast under the following conditions: 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.

RSTP supports rapid convergence. Like STP, it is of the following disadvantages: all bridges in a LAN are on the same spanning tree; redundant links cannot be blocked by VLAN; the packets of all VLANs are forwarded along the same spanning tree.

**MSTP Features**

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links.

MSTP features the following:
MSTP supports mapping VLANs to MST instances (MSTIs) by means of a VLAN-to-MSTI mapping table. MSTP introduces instance (integrates multiple VLANs into a set) and can bind multiple VLANs to an instance, thus saving communication overhead and improving resource utilization.

MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.

MSTP prunes a ring network into a network with tree topology, preventing packets from being duplicated and forwarded in a network endlessly. Furthermore, it offers multiple redundant paths for forwarding data, and thus achieves load balancing for forwarding VLAN data.

MSTP is compatible with STP and RSTP.

**Basic MSTP Terminologies**

Figure 72 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

**MST region**

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-MSTI mapping configuration and the same MSTP revision level.
A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands.

As shown in Figure 72, all the switches in region A0 are of the same MST region-related configuration, including:

- Region name
- VLAN-to-MSTI mapping (that is, VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to MSTI 2, and the other VLANs are mapped to CIST.)
- MSTP revision level (not shown in Figure 72)

**MSTI**
A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other. For example, each region in Figure 72 contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

**VLAN-to-MSTI mapping table**
A VLAN-to-MSTI mapping table is maintained for each MST region. The table is a collection of mappings between VLANs and MSTIs. For example, in Figure 72, the VLAN-to-MSTI mapping table of region A0 contains these mappings: VLAN 1 to MSTI 1; VLAN 2 to MSTI 2, and other VLANs to CIST. In an MST region, load balancing is implemented according to the VLAN-to-MSTI mapping table.

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

ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it is a branch of CIST in the MST region.

In Figure 72, each MST region has an IST, which is a branch of the CIST.

**CST**
A CST is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a switch, then the CST is the spanning tree generated by STP or RSTP running on the switches.

**CIST**
A CIST is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST.

In Figure 72, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.
Region root
A region root is the root of the IST or an MSTI in an MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots.

In region D0 shown in Figure 72, the region root of MSTI 1 is switch B, and the region root of MSTI 2 is switch C.

Common root bridge
The common root bridge is the root of the CIST. The common root bridge of the network shown in Figure 72 is a switch in region A0.

Port role
MSTP calculation involves the following port roles: root port, designated port, master port, boundary port, alternate port, and backup port.

■ A root port is used to forward packets to the root.
■ A designated port is used to forward packets to a downstream network segment or switch.
■ A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root. In the CST, the master port is the root port of the region, which is considered as a node. The master port is a special boundary port. It is a root port in the IST/CIST while a master port in the other MSTIs.
■ A boundary port is located on the boundary of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region.
■ An alternate port is a secondary port of a root port or master port and is used for rapid transition. With the root port or master port being blocked, the alternate port becomes the new root port or master port.
■ A backup port is the secondary port of a designated port and is used for rapid transition. With the designated port being blocked, the backup port becomes the new designated port fast and begins to forward data seamlessly. When two ports of an MSTP-enabled switch are interconnected, the switch blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

In Figure 73, switch A, switch B, switch C, and switch D form an MST region. Port 1 and port 2 on switch A connect upstream to the common root. Port 5 and port 6 on switch C form a loop. Port 3 and port 4 on switch D connect downstream to other MST regions. This figure shows the roles these ports play.

■ A port can play different roles in different MSTIs.
■ The role a boundary port plays in an MSTI is consistent with the role it plays in the CIST. The master port, which is a root port in the CIST while a master port in the other MSTIs, is an exception.
■ For example, in Figure 73, port 1 on switch A is a boundary port. It is a root port in the CIST while a master port in all the other MSTIs in the region.
MSTP Overview

Port state
In MSTP, a port can be in one of the following three states:

- **Forwarding state.** Ports in this state can forward user packets and receive/send BPDU packets.
- **Learning state.** Ports in this state can receive/send BPDU packets but do not forward user packets.
- **Discarding state.** Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. Table 164 lists possible combinations of port states and port roles.

### Table 164 Combinations of port states and port roles

<table>
<thead>
<tr>
<th>Port role/Port state</th>
<th>Root / master port</th>
<th>Designated port</th>
<th>Boundary port</th>
<th>Alternate port</th>
<th>Backup port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding</td>
<td>,åô</td>
<td>,åô</td>
<td>,åô</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Learning</td>
<td>,åô</td>
<td>,åô</td>
<td>,åô</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Discarding</td>
<td>,åô</td>
<td>,åô</td>
<td>,åô</td>
<td>,åô</td>
<td>,åô</td>
</tr>
</tbody>
</table>

Principle of MSTP
MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that the configuration BPDUs for MSTP carry the MSTP configuration information on the switches.

Calculate the CIST
Through comparing configuration BPDUs, the switch of the highest priority in the network is selected as the root of the CIST. In each MST region, an IST is calculated by MSTP. At the same time, MSTP regards each MST region as a switch to calculate the CSTs of the network. The CSTs, together with the ISTs, form the CIST of the network.
Calculate an MSTI
In an MST region, different MSTIs are generated for different VLANs based on the VLAN-to-MSTI mappings. Each spanning tree is calculated independently, in the same way as how STP/RSTP is calculated.

Implement STP algorithm
In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

1 Each switch sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another switch:
   ■ If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the switch discards the BPDU and does not change the configuration BPDU of the port.
   ■ If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the switch replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

2 Configuration BPDUs are compared as follows:
   ■ The smaller the root ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
   ■ For configuration BPDUs with the same root IDs, the path costs are compared. Suppose S is the sum of the root path costs and the corresponding path cost of the port. The less the S value is, the higher the priority of the configuration BPDU is.
   ■ For configuration BPDUs with both the same root ID and the same root path cost, the designated bridge ID, designated port ID, the ID of the receiving port are compared in turn.

3 A spanning tree is calculated as follows:
   ■ Determining the root bridge

Root bridges are selected by configuration BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.

   ■ Determining the root port

For each switch in a network, the port on which the configuration BPDU with the highest priority is received is chosen as the root port of the switch.

   ■ Determining the designated port

First, the switch calculates a designated port configuration BPDU for each of its ports using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the root path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the switch, and the ID of the designated port being replaced with that of the port.
The switch then compares the calculated configuration BPDU with the original configuration BPDU received from the corresponding port on another switch. If the latter takes precedence over the former, the switch blocks the local port and keeps the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the switch sets the local port to the designated port, replaces the original configuration BPDU of the port with the calculated one and advertises it regularly.

**MSTP Implementation on Switches**

MSTP is compatible with both STP and RSTP. That is, MSTP-enabled switches can recognize the protocol packets of STP and RSTP and use them for spanning tree calculation. In addition to the basic MSTP functions, 3Com series switches also provide the following functions for users to manage their switches.

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU attack guard
- BPDU packet drop

**STP-related Standards**

STP-related standards include the following.

- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

**Configuring Root Bridge**

Table 165 lists the tasks to configure a root bridge.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MSTP</td>
<td>Required</td>
<td>“Enabling MSTP”</td>
</tr>
<tr>
<td></td>
<td>To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.</td>
<td></td>
</tr>
<tr>
<td>Configure an MST region</td>
<td>Required</td>
<td>“Configuring an MST Region”</td>
</tr>
<tr>
<td>Specify the current switch as a root bridge/secondary root bridge</td>
<td>Required</td>
<td>“Specifying the Current Switch as a Root Bridge/Secondary Root Bridge”</td>
</tr>
<tr>
<td>Configure the bridge priority of the current switch</td>
<td>Optional</td>
<td>“Configuring the Bridge Priority of the Current Switch”</td>
</tr>
<tr>
<td></td>
<td>The priority of a switch cannot be changed after the switch is specified as the root bridge or a secondary root bridge.</td>
<td></td>
</tr>
</tbody>
</table>
In a network containing switches with both GVRP and MSTP enabled, GVRP messages travel along the CIST. If you want to advertise a VLAN through GVRP, be sure to map the VLAN to the CIST (MSTI 0) when configuring the VLAN-to-MSTI mapping table.

**Configuration Prerequisites**

The role (root, branch, or leaf) of each switch in each MSTI is determined.

**Configuring an MST Region**

**Table 166  Configure an MST region**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the mode a port recognizes and sends MSTP packets</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the MSTP operation mode</td>
<td>stp region-configuration</td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum hop count of an MST region</td>
<td>region-name name</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the maximum hop count of an MST region</td>
<td>instance instance-id vlan</td>
<td>Required, The default MST region name of a switch is its MAC address.</td>
</tr>
<tr>
<td></td>
<td>vlan-list</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the VLAN-to-MSTI mapping table for the MST region</td>
<td>vlan-mapping modulo modulo</td>
<td>Both commands can be used to configure VLAN-to-MSTI mapping tables.</td>
</tr>
</tbody>
</table>

By default, all VLANs in an MST region are mapped to MSTI 0.
NTDP packets sent by devices in a cluster can only be transmitted within the MSTI where the management VLAN of the cluster resides.

Configuring MST region-related parameters (especially the VLAN-to-MSTI mapping table) results in spanning tree recalculation and network topology jitter. To reduce network topology jitter caused by the configuration, MSTP does not recalculate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really take effect:

- Activate the new MST region-related settings by using the `active region-configuration` command
- Enable MSTP by using the `stp enable` command
- MSTP-enabled switches are in the same region only when they have the same format selector (a 802.1s-defined protocol selector, which is 0 by default and cannot be configured), MST region name, VLAN-to-MSTI mapping table, and revision level.
- The Switch 5500 Family supports only the MST region name, VLAN-to-MSTI mapping table, and revision level. Switches with the settings of these parameters being the same are assigned to the same MST region.

### Configuration example

# Configure an MST region, named `info`, the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to MSTI 1, and VLAN 20 through VLAN 30 being mapped to MSTI 2.

```
<5500> system-view
[5500] stp region-configuration
[5500-mst-region] region-name info
[5500-mst-region] instance 1 vlan 2 to 10
[5500-mst-region] instance 2 vlan 20 to 30
[5500-mst-region] revision-level 1
[5500-mst-region] active region-configuration
```

# Verify the above configuration.

```
[5500-mst-region] check region-configuration
```

Admin configuration

Format selector : 0
**Specifying the Current Switch as a Root Bridge/Secondary Root Bridge**

MSTP can automatically choose a switch as a root bridge through calculation. You can also manually specify the current switch as a root bridge by using the corresponding commands.

### Specify the current switch as the root bridge of a spanning tree

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the current switch as the root bridge of a spanning tree</td>
<td>stp [ instance instance-id ] root primary [ bridge-diameter bridgenumber ] [ hello-time centi-seconds ]</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Specify the current switch as the secondary root bridge of a spanning tree

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the current switch as the secondary root bridge of a specified spanning tree</td>
<td>stp [ instance instance-id ] root secondary [ bridge-diameter bridgenumber ] [ hello-time centi-seconds ]</td>
<td>Required</td>
</tr>
</tbody>
</table>

Using the `stp root primary/stp root secondary` command, you can specify the current switch as the root bridge or the secondary root bridge of the MSTI identified by the `instance-id` argument. If the value of the `instance-id` argument is set to 0, the `stp root primary/stp root secondary` command specify the current switch as the root bridge or the secondary root bridge of the CIST.

A switch can play different roles in different MSTIs. That is, it can be the root bridges in an MSTI and be a secondary root bridge in another MSTI at the same time. But in the same MSTI, a switch cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for a MSTI, the one with the smallest MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the hello time parameters while configuring a root bridge/secondary root bridge. Refer to “Configuring the Network Diameter of the Switched Network” on page 248 and “Configuring the Timeout Time Factor” on page 250 for information about the network diameter parameter and the hello time parameter.
You can configure a switch as the root bridges of multiple MSTIs. But you cannot configure two or more root bridges for one MSTI. So, do not configure root bridges for the same MSTI on two or more switches using the `stp root primary` command.

You can configure multiple secondary root bridges for one MSTI. That is, you can configure secondary root bridges for the same MSTI on two or more switches using the `stp root secondary` command.

You can also configure the current switch as the root bridge by setting the priority of the switch to 0. Note that once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Configuration example

```
# Configure the current switch as the root bridge of MSTI 1 and a secondary root bridge of MSTI 2.

<5500> system-view
[5500] stp instance 1 root primary
[5500] stp instance 2 root secondary
```

**Configuring the Bridge Priority of the Current Switch**

Root bridges are selected according to the bridge priorities of switches. You can make a specific switch be selected as a root bridge by setting a lower bridge priority for the switch. An MSTP-enabled switch can have different bridge priorities in different MSTIs.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Set the bridge priority for the</td>
<td>`stp [instance instance-id]</td>
<td>Required</td>
</tr>
<tr>
<td>current switch</td>
<td>priority priority`</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default bridge priority of a switch is 32,768.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- Once you specify a switch as the root bridge or a secondary root bridge by using the `stp root primary` or `stp root secondary` command, the bridge priority of the switch cannot be configured any more.

- During the selection of the root bridge, if multiple switches have the same bridge priority, the one with the smallest MAC address becomes the root bridge.

**Configuration example**

```
# Set the bridge priority of the current switch to 4,096 in MSTI 1.

<5500> system-view
[5500] stp instance 1 priority 4096
```

**Configuring How a Port Recognizes and Sends MSTP Packets**

A port can be configured to recognize and send MSTP packets in the following modes.

- Automatic mode. Ports in this mode determine the format of the MSTP packets to be sent according to the format of the received packets.
- Legacy mode. Ports in this mode recognize/send packets in legacy format.
- 802.1s mode. Ports in this mode recognize/send packets in dot1s format.

A port acts as follows according to the format of MSTP packets forwarded by a peer switch or router.

When a port operates in the automatic mode:

- The port automatically determines the format (legacy or dot1s) of received MSTP packets and then determines the format of the packets to be sent accordingly, thus communicating with the peer devices.
- If the format of the received packets changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be brought up by the network administrator.

When a port operates in the legacy mode:

- The port recognizes and sends MSTP packets in legacy format. In this case, the port can only communicate with the peer through packets in legacy format.
- If packets in dot1s format are received, the port turns to discarding state to prevent network storm.

When a port operates in the 802.1s mode:

- The port only recognizes and sends MSTP packets in dot1s format. In this case, the port can only communicate with the peer through packets in dot1s format.
- If packets in legacy format are received, the port turns to discarding state to prevent network storm.

**Configuration procedure**

**Table 170** Configure the mode a port recognizes and sends MSTP packets (in system view)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure how a port recognizes and sends MSTP packets</td>
<td>stp interface interface-type interface-number compliance { auto</td>
<td>dot1s</td>
</tr>
</tbody>
</table>
|                                        |                                          | By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

**Table 171** Configure the mode a port recognizes and sends MSTP packets (in Ethernet port view)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 171  Configure the mode a port recognizes and sends MSTP packets (in Ethernet port view)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure how a port recognizes and sends MSTP packets</td>
<td>stp compliance { auto</td>
<td>dot1s</td>
</tr>
</tbody>
</table>

Table 172  Configure the MSTP operation mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the MSTP operation mode</td>
<td>stp mode { stp</td>
<td>rstp</td>
</tr>
</tbody>
</table>

Configuration example

# Specify the MSTP operation mode as STP-compatible.

<5500> system-view
[5500] stp mode stp

To make an MSTP-enabled switch compatible with STP/RSTP, MSTP provides the following three operation modes:

- STP-compatible mode, where the ports of a switch send STP BPDUs to neighboring devices. If STP-enabled switches exist in a switched network, you can use the stp mode stp command to configure an MSTP-enabled switch to operate in STP-compatible mode.

- RSTP-compatible mode, where the ports of a switch send RSTP BPDUs to neighboring devices. If RSTP-enabled switches exist in a switched network, you can use the stp mode rstp command to configure an MSTP-enabled switch to operate in RSTP-compatible mode.

- MSTP mode, where the ports of a switch send MSTP BPDUs or STP BPDUs (if the switch is connected to STP-enabled switches) to neighboring devices. In this case, the switch is MSTP-capable.
Configuring the Maximum Hop Count of an MST Region

The maximum hop count configured on the region root is also the maximum hops of the MST region. The value of the maximum hop count limits the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in an MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes one switch. Such a mechanism disables the switches that are beyond the maximum hop count from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hop count configured on the switch operating as the root bridge of the CIST or an MSTI in an MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in the MST region adopt the maximum hop settings of their root bridges.

Configuration procedure

Table 173 Configure the maximum hop count for an MST region

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum hop count of</td>
<td>stp max-hops</td>
<td>Required</td>
</tr>
<tr>
<td>the MST region</td>
<td>hops</td>
<td>By default, the maximum hop count of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>an MST region is 20.</td>
</tr>
</tbody>
</table>

The bigger the maximum hop count, the larger the MST region is. Note that only the maximum hop settings on the switch operating as a region root can limit the size of the MST region.

Configuration example

# Configure the maximum hop count of the MST region to be 30.

```
<5500> system-view
[5500] stp max-hops 30
```

Configuring the Network Diameter of the Switched Network

In a switched network, any two switches can communicate with each other through a specific path made up of multiple switches. The network diameter of a network is measured by the number of switches; it equals the number of the switches on the longest path (that is, the path containing the maximum number of switches).

Configuration procedure

Table 174 Configure the network diameter of the switched network

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the network diameter of</td>
<td>stp bridge-diameter</td>
<td>Required</td>
</tr>
<tr>
<td>the switched network</td>
<td>bridgenumber</td>
<td>The default network diameter of a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network is 7.</td>
</tr>
</tbody>
</table>
The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, an MSTP-enabled switch adjusts its hello time, forward delay, and max age settings accordingly to better values.

The network diameter setting only applies to CIST; it is invalid for MSTIs.

**Configuration example**

```plaintext
# Configure the network diameter of the switched network to 6.
<5500> system-view
[5500] stp bridge-diameter 6
```

**Configuring the MSTP Time-related Parameters**

Three MSTP time-related parameters exist: forward delay, hello time, and max age. You can configure the three parameters to control the process of spanning tree calculation.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Table 175</th>
<th>Configure MSTP time-related parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Configure the forward delay parameter</td>
<td>stp timer forward-delay centiseconds</td>
</tr>
<tr>
<td>Configure the hello time parameter</td>
<td>stp timer hello centiseconds</td>
</tr>
<tr>
<td>Configure the max age parameter</td>
<td>stp timer max-age centiseconds</td>
</tr>
</tbody>
</table>

All switches in a switched network adopt the three time-related parameters configured on the CIST root bridge.

**CAUTION:**

- The forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large forward delay. A too small forward delay parameter may result in temporary redundant paths. And a too large forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default value is recommended.

- An adequate hello time parameter enables a switch to detect link failures in time without occupying too many network resources. And a too small hello time parameter may result in duplicated configuration BPDUs being sent.
frequently, which increases the work load of the switches and wastes network resources. The default value is recommended.

- As for the max age parameter, if it is too small, network congestion may be falsely regarded as link failures, which results in frequent spanning tree recalculation. If it is too large, link problems may be unable to be detected in time, which prevents spanning trees being recalculated in time and makes the network less adaptive. The default value is recommended.

As for the configuration of the three time-related parameters (that is, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay - 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the `stp root primary` or `stp root secondary` command. After that, the three proper time-related parameters are determined automatically.

**Configuration example**

# Configure the forward delay parameter to be 1,600 centiseconds, the hello time parameter to be 300 centiseconds, and the max age parameter to be 2,100 centiseconds (assuming that the current switch operates as the CIST root bridge).

```
<5500> system-view
[5500] stp timer forward-delay 1600
[5500] stp timer hello 300
[5500] stp timer max-age 2100
```

### Configuring the Timeout Time Factor

When the network topology is stable, a non-root-bridge switch regularly forwards BPDUs received from the root bridge to its neighboring devices at the interval specified by the hello time parameter to check link failures. Normally, a switch regards its upstream switch faulty if the former does not receive any BPDU from the latter in a period three times of the hello time and then initiates the spanning tree recalculation process.

Spanning trees may be recalculated even in a steady network if an upstream switch continues to be busy. You can configure the timeout time factor to a larger number to avoid such cases. Normally, the timeout time can be four or more times of the hello time. For a steady network, the timeout time can be five to seven times of the hello time.

### Configuration procedure

**Table 176**  Configure the timeout time factor

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure the timeout time factor for the switch</td>
<td>stp timer-factor number</td>
<td>Required  The timeout time factor defaults to 3.</td>
</tr>
</tbody>
</table>
For a steady network, the timeout time can be five to seven times of the hello time.

**Configuration example**

```
# Configure the timeout time factor to be 6.
<5500> system-view
[5500] stp timer-factor 6
```

The maximum transmitting rate of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the hello time parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

**Configure the maximum transmitting rate for specified ports in system view**

**Table 177** Configure the maximum transmitting rate for specified ports in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum transmitting rate for specified ports</td>
<td>stp interface interface-list transmit-limit packetnum</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.</td>
</tr>
</tbody>
</table>

**Configure the maximum transmitting speed in Ethernet port view**

**Table 178** Configure the maximum transmitting rate in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum transmitting rate</td>
<td>stp transmit-limit packetnum</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.</td>
</tr>
</tbody>
</table>

As the maximum transmitting rate parameter determines the number of the configuration BPDUs transmitted in each hello time, set it to a proper value to prevent MSTP from occupying too many network resources. The default value is recommended.

**Configuration example**

```
# Set the maximum transmitting rate of Ethernet 1/0/1 to 15.
1 Configure the maximum transmitting rate in system view

<5500> system-view
[5500] stp interface Ethernet 1/0/1 transmit-limit 15

2 Configure the maximum transmitting rate in Ethernet port view

<5500> system-view
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] stp transmit-limit 15
```
Configuring the Current Port as an Edge Port

Edge ports are ports that neither directly connects to other switches nor indirectly connects to other switches through network segments. After a port is configured as an edge port, the rapid transition mechanism is applicable to the port. That is, when the port changes from the blocking state to the forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in one of the following two ways.

**Configure a port as an edge port in system view**

<table>
<thead>
<tr>
<th>Table 179</th>
<th>Configure a port as an edge port in system view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Configure the specified ports as edge ports</td>
<td>stp interface interface-list edged-port enable</td>
</tr>
</tbody>
</table>

By default, all the Ethernet ports of a switch are non-edge ports.

**Configure a port as an edge port in Ethernet port view**

<table>
<thead>
<tr>
<th>Table 180</th>
<th>Configure a port as an edge port in Ethernet port view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the port as an edge port</td>
<td>stp edged-port enable</td>
</tr>
</tbody>
</table>

By default, all the Ethernet ports of a switch are non-edge ports.

On a switch with BPDU guard disabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.

You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU guard function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

**Configuration example**

# Configure Ethernet 1/0/1 as an edge port.

1 Configure Ethernet 1/0/1 as an edge port in system view

   `<5500> system-view
   [5500] stp interface Ethernet 1/0/1 edged-port enable`

2 Configure Ethernet 1/0/1 as an edge port in Ethernet port view

   `<5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet 1/0/1] stp edged-port enable`
Specifying Whether the Link Connected to a Port Is Point-to-point Link

A point-to-point link directly connects two switches. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can turn to the forwarding state rapidly by exchanging synchronization packets, thus reducing the forward delay.

You can determine whether or not the link connected to a port is a point-to-point link in one of the following two ways.

Specify whether the link connected to a port is point-to-point link in system view

Table 181  Specify whether the link connected to a port is point-to-point link in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify whether the link connected to a port is point-to-point link</td>
<td>stp interface interface-list point-to-point { force-true</td>
<td>force-false</td>
</tr>
</tbody>
</table>

Specify whether the link connected to a port is point-to-point link in Ethernet port view

Table 182  Specify whether the link connected to a port is point-to-point link in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Specify whether the link connected to a port is a point-to-point link</td>
<td>stp point-to-point { force-true</td>
<td>force-false</td>
</tr>
</tbody>
</table>

- Among aggregated ports, you can only configure the links of master ports as point-to-point links.
- If an auto-negotiating port operates in full duplex mode after negotiation, you can configure the link of the port as a point-to-point link.

After you configure the link of a port as a point-to-point link, the configuration applies to all the MSTIs the port belongs to. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, loops may occur temporarily.

Configuration example

# Configure the link connected to Ethernet 1/0/1 as a point-to-point link.

1 Perform this configuration in system view

   <5500> system-view
   [5500] stp interface Ethernet 1/0/1 point-to-point force-true

2 Perform this configuration in Ethernet port view

   <5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] stp point-to-point force-true
Enabling MSTP

Configuration procedure

<table>
<thead>
<tr>
<th>Table 183</th>
<th>Enable MSTP in system view</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable MSTP</td>
<td>stp enable</td>
</tr>
<tr>
<td>Disable MSTP on specified ports</td>
<td>stp interface interface-list disable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 184</th>
<th>Enable MSTP in Ethernet port view</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable MSTP</td>
<td>stp enable</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Disable MSTP on the port</td>
<td>stp disable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other MSTP-related settings can take effect only after MSTP is enabled on the switch.

Configuration example

# Enable MSTP on the switch and disable MSTP on Ethernet 1/0/1.

1. Perform this configuration in system view
   
   `<5500> system-view
   [5500] stp enable
   [5500] stp interface Ethernet 1/0/1 disable`

2. Perform this configuration in Ethernet port view
   
   `<5500> system-view
   [5500] stp enable`
Table 185 lists the tasks to configure a leaf node.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MSTP</td>
<td>To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.</td>
<td>“Enabling MSTP”</td>
</tr>
<tr>
<td>Configure the MST region</td>
<td>Required</td>
<td>“Configuring an MST Region”</td>
</tr>
<tr>
<td>Configure the mode a port recognizes and sends MSTP packets</td>
<td>Optional</td>
<td>“Configuring How a Port Recognizes and Sends MSTP Packets”</td>
</tr>
<tr>
<td>Configure the timeout time factor</td>
<td>Optional</td>
<td>“Configuring the Timeout Time Factor”</td>
</tr>
<tr>
<td>Configure the maximum transmitting speed on the current port</td>
<td>Optional, The default value is recommended.</td>
<td>“Configuring the Maximum Transmitting Rate on the Current Port”</td>
</tr>
<tr>
<td>Configure the current port as an edge port</td>
<td>Optional</td>
<td>“Configuring the Current Port as an Edge Port”</td>
</tr>
<tr>
<td>Configure the path cost for a port</td>
<td>Optional</td>
<td>“Configuring the Path Cost for a Port”</td>
</tr>
<tr>
<td>Configure the port priority</td>
<td>Optional</td>
<td>“Configuring Port Priority”</td>
</tr>
<tr>
<td>Specify whether the link connected to a port is point-to-point link</td>
<td>Optional</td>
<td>“Specifying Whether the Link Connected to a Port Is Point-to-point Link”</td>
</tr>
</tbody>
</table>

In a network containing switches with both GVRP and MSTP enabled, GVRP messages travel along the CIST. If you want to advertise a VLAN through GVRP, be sure to map the VLAN to the CIST (MSTI 0) when configuring the VLAN-to-MSTI mapping table.

Configuration Prerequisites

The role (root, branch, or leaf) of each switch in each MSTI is determined.

Configuring the MST Region

Refer to “Configuring an MST Region” on page 242.

Configuring the Mode a Port Recognizes and Sends MSTP Packets

Refer to “Configuring How a Port Recognizes and Sends MSTP Packets” on page 245.

Configuring the Timeout Time Factor

Refer to “Configuring the Timeout Time Factor” on page 250.

[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] stp disable
CHAPTER 26: MSTP CONFIGURATION

Configuring the Maximum Transmitting Speed on the Current Port

Refer to “Configuring the Maximum Transmitting Rate on the Current Port” on page 251.

Configuring a Port as an Edge Port

Refer to “Configuring the Current Port as an Edge Port” on page 252.

Configuring the Path Cost for a Port

The path cost parameter reflects the rate of the link connected to the port. For a port on an MSTP-enabled switch, the path cost may be different in different MSTIs. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that VLAN-based load balancing can be implemented.

Path cost of a port can be determined by the switch or through manual configuration.

Standards for calculating path costs of ports

Currently, a switch can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.
- **legacy**: Adopts the proprietary standard to calculate the default path costs of ports.

<table>
<thead>
<tr>
<th>Table 186</th>
<th>Specify the standard for calculating path costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>Specify the standard for calculating the default path costs of the links connected to the ports of the switch</td>
<td><strong>stp pathcost-standard</strong></td>
</tr>
<tr>
<td></td>
<td>**{dot1d-1998</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 187</th>
<th>Transmission speeds and the corresponding path costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmission rate</strong></td>
<td><strong>Operation mode (half-/full-duplex)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>Half-duplex/Full-duplex</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 2 ports</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 3 ports</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 4 ports</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Half-duplex/Full-duplex</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 2 ports</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 3 ports</td>
</tr>
<tr>
<td></td>
<td>Aggregated link 4 ports</td>
</tr>
</tbody>
</table>
Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

\[
\text{Path cost} = \frac{200,000}{\text{link transmission rate}},
\]

where \text{link transmission rate} is the sum of the rates of all the unblocked ports on the aggregated link measured in 100 Kbps.

### Configure the path cost for specific ports

**Table 188** Configure the path cost for specified ports in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>System-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the path cost for</td>
<td>stp interface interface-list [ instance</td>
<td>Required</td>
</tr>
<tr>
<td>specified ports</td>
<td>instance-id ] cost</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>An MSTP-enabled switch can calculate path costs for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all its ports automatically.</td>
</tr>
</tbody>
</table>

**Table 189** Configure the path cost for a port in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>System-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the path cost for the</td>
<td>stp [ instance instance-id ] cost</td>
<td>Required</td>
</tr>
<tr>
<td>port</td>
<td></td>
<td>An MSTP-enabled switch can calculate path costs for all its ports automatically.</td>
</tr>
</tbody>
</table>

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the `stp cost` command with the `instance-id` argument being 0 sets the path cost on the CIST for the port.
Configuration example (A)
# Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be 2,000.

1 Perform this configuration in system view
   <5500> system-view
   [5500] stp interface Ethernet 1/0/1 instance 1 cost 2000

2 Perform this configuration in Ethernet port view
   <5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] stp instance 1 cost 2000

Configuration example (B)
# Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be calculated by the
MSTP-enabled switch according to the IEEE 802.1D-1998 standard.

1 Perform this configuration in system view
   <5500> system-view
   [5500] undo stp interface Ethernet 1/0/1 instance 1 cost
   [5500] stp pathcost-standard dot1d-1998

2 Perform this configuration in Ethernet port view
   <5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] undo stp instance 1 cost
   [5500-Ethernet1/0/1] quit
   [5500] stp pathcost-standard dot1d-1998

Configuring Port Priority

Port priority is an important criterion on determining the root port. In the same
condition, the port with the smallest port priority value becomes the root port.

A port on an MSTP-enabled switch can have different port priorities and play
different roles in different MSTIs. This enables packets of different VLANs to be
forwarded along different physical paths, so that VLAN-based load balancing can
be implemented.

You can configure port priority in one of the following two ways.

Configure port priority in system view

<table>
<thead>
<tr>
<th>Table 190</th>
<th>Configure port priority in system view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Configure port priority for specified ports</td>
<td>stp interface interface-list instance instance-id port priority priority</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure port priority in Ethernet port view

<table>
<thead>
<tr>
<th>Table 191</th>
<th>Configure port priority in Ethernet port view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
</tbody>
</table>
Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree recalculation.

You can configure port priorities according to actual networking requirements.

**Configuration example**

# Configure the port priority of Ethernet1/0/1 in MSTI 1 to be 16.

1. Perform this configuration in system view

   `<5500> system-view
   [5500] stp interface Ethernet 1/0/1 instance 1 port priority 16`

2. Perform this configuration in Ethernet port view

   `<5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] stp instance 1 port priority 16`

Specifying Whether the Link Connected to a Port Is a Point-to-point Link

Refer to “Specifying Whether the Link Connected to a Port Is Point-to-point Link” on page 253.

Enabling MSTP

Refer to “Enabling MSTP” on page 254.

Performing mCheck Operation

Ports on an MSTP-enabled switch can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

A port on an MSTP-enabled switch operating as an upstream switch transits to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP-enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, a port on an RSTP-enabled switch operating as an upstream switch turns to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP-compatible mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP-compatible mode by performing the mCheck operation on the port.
**Configuration Prerequisites**

MSTP runs normally on the switch.

**Configuration Procedure**

You can perform the mCheck operation in the following two ways.

### Perform the mCheck operation in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Perform the mCheck operation</td>
<td>stp [ interface interface-list ] mcheck</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Perform the mCheck operation in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Perform the mCheck operation</td>
<td>stp mcheck</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuration Example**

# Perform the mCheck operation on Ethernet 1/0/1.

1. Perform this configuration in system view

   `<5500> system-view
   [5500] stp interface Ethernet 1/0/1 mcheck`

2. Perform this configuration in Ethernet port view

   `<5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] stp mcheck`

**Configuring Guard Functions**

**Introduction**

The following guard functions are available on an MSTP-enabled switch: BPDU guard, root guard, loop guard, TC-BPDU attack guard, and BPDU drop.

**BPDU guard**

Normally, the access ports of the devices operating on the access layer are directly connected to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning tree recalculation and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU guard function. With this function enabled on a switch, the switch shuts down the
edge ports that receive configuration BPDUs and then reports these cases to the administrator. Ports shut down in this way can only be restored by the administrator.

**Root guard**
A root bridge and its secondary root bridges must reside in the same region. The root bridge of the CIST and its secondary root bridges are usually located in the high-bandwidth core region. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this problem by utilizing the root guard function. Ports with this function enabled can only be kept as designated ports in all MSTIs. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state (rather than become a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

**Loop guard**
A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions or unidirectional link failures. If a switch does not receive BPDUs from the upstream switch for certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports turns to the forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or unidirectional link failures occur, both the root port and the blocked ports become designated ports and turn to the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.

**CAUTION:** With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

**TC-BPDU attack guard**
Normally, a switch removes its MAC address table and ARP entries upon receiving TC-BPDUs. If a malicious user sends a large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing the MAC address table and ARP entries, which may affect spanning tree calculation, occupy large amount of bandwidth and increase switch CPU utilization.

With the TC-BPDU attack guard function enabled, a switch performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the switch only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a switch from being busy in removing the MAC address table and ARP entries.

You can use the `stp tc-protection threshold` command to set the maximum times for a switch to remove the MAC address table and ARP entries in a specific period. When the number of the TC-BPDUs received within a period is less than
the maximum times, the switch performs a removing operation upon receiving a TC-BPDU. After the number of the TC-BPDUs received reaches the maximum times, the switch stops performing the removing operation. For example, if you set the maximum times for a switch to remove the MAC address table and ARP entries to 100 and the switch receives 200 TC-BPDUs in the period, the switch removes the MAC address table and ARP entries for only 100 times within the period.

**BPDU dropping**

In a STP-enabled network, some users may send BPDU packets to the switch continuously in order to destroy the network. When a switch receives the BPDU packets, it will forward them to other switches. As a result, STP calculation is performed repeatedly, which may occupy too much CPU of the switches or cause errors in the protocol state of the BPDU packets.

In order to avoid this problem, you can enable BPDU dropping on Ethernet ports. Once the function is enabled on a port, the port will not receive or forward any BPDU packets. In this way, the switch is protected against the BPDU packet attacks so that the STP calculation is assured to be right.

**Configuration Prerequisites**

MSTP runs normally on the switch.

### Configuring BPDU Guard

**Configuration procedure**

<table>
<thead>
<tr>
<th>Table 194 Configure BPDU guard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Enable the BPDU guard function</td>
</tr>
</tbody>
</table>

The BPDU guard function is disabled by default.

**Configuration example**

# Enable the BPDU guard function.

```
<5500> system-view
[5500] stp bpdu-protection
```

⚠️ **CAUTION:** As Gigabit ports of a Switch 5500 cannot be shut down, the BPDU guard function is not applicable to these ports even if you enable the BPDU guard function and specify these ports to be MSTP edge ports. This does not apply to the Switch 5500G.

### Configuring Root Guard

**Configuration procedure**

<table>
<thead>
<tr>
<th>Table 195 Configure the root guard function in system view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Enable the root guard function on specified ports</td>
</tr>
</tbody>
</table>

The root guard function is disabled by default.
Configuring Guard Functions

### Configuration example

1. Perform this configuration in system view

   ```
   <5500> system-view
   [5500] stp interface Ethernet 1/0/1 root-protection
   ```

2. Perform this configuration in Ethernet port view

   ```
   <5500> system-view
   [5500] interface Ethernet 1/0/1
   [5500-Ethernet1/0/1] stp root-protection
   ```

### Configuring Loop Guard

#### Configuration procedure

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable the loop guard function on the current port</td>
<td>stp loop-protection</td>
<td>Required</td>
</tr>
</tbody>
</table>

The loop guard function is disabled by default.

#### Configuration example

# Enable the loop guard function on Ethernet 1/0/1.

```
<5500> system-view
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] stp loop-protection
```
CHAPTER 26: MSTP CONFIGURATION

Configuration example

# Enable the TC-BPDU attack guard function

<5500> system-view  
[5500] stp tc-protection enable

# Set the maximum times for the switch to remove the MAC address table and ARP entries within each 10 seconds to 5.

<5500> system-view  
[5500] stp tc-protection threshold 5

Configuring BPDU Dropping

Table 199  Configure BPDU dropping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-name</td>
<td>—</td>
</tr>
<tr>
<td>Enable BPDU dropping</td>
<td>bpdu-drop any</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BPDU dropping is disabled by default.</td>
</tr>
</tbody>
</table>

# Enable BPDU dropping on Ethernet 1/0/1.

<5500>system-view  
[5500] interface Ethernet 1/0/1  
[5500-Ethernet1/0/1] bpdu-drop any

Configuring Digest Snooping

Introduction

According to IEEE 802.1s, two interconnected switches can communicate with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP-enabled switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some other manufacturers’ switches adopt proprietary spanning tree protocols, they cannot communicate with the other switches in an MST region even if they are configured with the same MST region-related settings as the other switches in the MST region.

This problem can be overcome by implementing the digest snooping feature. If a port on a Switch 5500 is connected to another manufacturer’s switch that has the same MST region-related configuration as its own but adopts a proprietary
spanning tree protocol, you can enable digest snooping on the port. Then the Switch 5500 regards another manufacturer’s switch as in the same region; it records the configuration digests carried in the BPDUs received from another manufacturer’s switch, and put them in the BPDUs to be sent to the other manufacturer’s switch. In this way, the Switch 5500 can communicate with another manufacturer’s switches in the same MST region.

**CAUTION:** The digest snooping function is not applicable to edge ports.

**Configuring Digest Snooping**

Configure the digest snooping feature on a switch to enable it to communicate with other switches adopting proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

**Configuration prerequisites**

The switch to be configured is connected to another manufacturer’s switch adopting a proprietary spanning tree protocol. MSTP and the network operate normally.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable the digest snooping feature</td>
<td>stp config-digest-snooping</td>
<td>Required The digest snooping feature is disabled on a port by default.</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enable the digest snooping feature globally</td>
<td>stp config-digest-snooping</td>
<td>Required The digest snooping feature is disabled globally by default.</td>
</tr>
<tr>
<td>Display the current configuration</td>
<td>display current-configuration</td>
<td>You can execute this command in any view.</td>
</tr>
</tbody>
</table>

- **When the digest snooping feature is enabled on a port, the port state turns to the discarding state. That is, the port will not send BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.**

- **The digest snooping feature is needed only when your switch is connected to another manufacturer’s switches adopting proprietary spanning tree protocols.**

- **To enable the digest snooping feature successfully, you must first enable it on all the ports of your switch that are connected to another manufacturer’s switches adopting proprietary spanning tree protocols and then enable it globally.**

- **To enable the digest snooping feature, the interconnected switches and another manufacturer’s switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).**
The digest snooping feature must be enabled on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols in the same MST region.

When the digest snooping feature is enabled globally, the VLAN-to-MSTI mapping table cannot be modified.

The digest snooping feature is not applicable to boundary ports in an MST region.

The digest snooping feature is not applicable to edge ports in an MST region.

### Configuring Rapid Transition

**Introduction**

Designated ports of RSTP-enabled or MSTP-enabled switches use the following two types of packets to implement rapid transition:

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

Both RSTP and MSTP specify that the upstream switch can perform rapid transition operation on the designated port only when the port receives an agreement packet from the downstream switch. The difference between RSTP and MSTP are:

- For MSTP, the upstream switch sends agreement packets to the downstream switch; and the downstream switch sends agreement packets to the upstream switch only after it receives agreement packets from the upstream switch.
- For RSTP, the upstream switch does not send agreement packets to the downstream switch.

Figure 74 and Figure 75 illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

**Figure 74** The RSTP rapid transition mechanism
The cooperation between MSTP and RSTP is limited in the process of rapid transition. For example, when the upstream switch adopts RSTP, the downstream switch adopts MSTP and the downstream switch does not support RSTP-compatible mode, the root port on the downstream switch receives no agreement packet from the upstream switch and thus sends no agreement packets to the upstream switch. As a result, the designated port of the upstream switch fails to transit rapidly and can only turn to the forwarding state after a period twice the forward delay.

Some other manufacturers’ switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operating as the upstream switch connects with a 3Com series switch running MSTP, the upstream designated port fails to change its state rapidly.

The rapid transition feature is developed to resolve this problem. When a 3Com series switch running MSTP is connected in the upstream direction to another manufacturer’s switch running proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the 3Com series switch operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

**Configuring Rapid Transition**

**Configuration prerequisites**

As shown in Figure 76, a 3Com series switch is connected to another manufacturer’s switch. The former operates as the downstream switch, and the latter operates as the upstream switch. The network operates normally.

The upstream switch is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is the designated port.

The downstream switch is running MSTP. Port 2 is the root port.
CHAPTER 26: MSTP CONFIGURATION

Figure 76  Network diagram for rapid transition configuration

Another manufacturer's switch

Port 1

Port 2

Configuration procedure

1  Configure the rapid transition feature in system view

Table 201  Configure the rapid transition feature in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the rapid transition feature</td>
<td>stp interface interface-type interface-number no-agreement-check</td>
<td>Required By default, the rapid transition feature is disabled on a port.</td>
</tr>
</tbody>
</table>

2  Configure the rapid transition feature in Ethernet port view

Table 202  Configure the rapid transition feature in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable the rapid transition feature</td>
<td>stp no-agreement-check</td>
<td>Required By default, the rapid transition feature is disabled on a port.</td>
</tr>
</tbody>
</table>

- The rapid transition feature can be enabled on only root ports or alternate ports.
- If you configure the rapid transition feature on a designated port, the feature does not take effect on the port.

Configuring VLAN-VPN Tunnel

Introduction  The VLAN-VPN Tunnel function enables STP packets to be transparently transmitted between geographically dispersed customer networks through specified VLAN VPNs in service provider networks, through which spanning trees
can be generated across these customer networks and are independent of those of the service provider network.

As shown in Figure 77, the upper part is the service provider network, and the lower part comprises the customer networks. The service provider network comprises packet input/output devices, and the customer network has networks A and B. On the service provider network, configure the arriving STP packets at the input device to have MAC addresses in a special format, and reconvert them back to their original formats at the output device. This is how transparent transmission is implemented over the service provider network.

Figure 77 VLAN-VPN tunnel network hierarchy

![VLAN-VPN tunnel network hierarchy](image)

<table>
<thead>
<tr>
<th>Table 203</th>
<th>Configure VLAN-VPN tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable MSTP globally</td>
<td>stp enable</td>
</tr>
<tr>
<td>Enable the VLAN-VPN tunnel function globally</td>
<td>vlan-vpn tunnel</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
</tr>
<tr>
<td>Enable the VLAN VPN function for the Ethernet port</td>
<td>vlan-vpn enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- The VLAN-VPN tunnel function can be enabled on STP-enabled devices only.
To enable the VLAN-VPN tunnel function, make sure the links between service provider networks are trunk links.

If a fabric port exists on a switch, you cannot enable the VLAN VPN function on any port of the switch.

**STP Maintenance Configuration**

**Introduction**

In a large-scale network with MSTP enabled, there may be many MSTP instances, and so the status of a port may change frequently. In this case, maintenance personnel may expect that log/trap information is output to the log host when particular ports fail, so that they can check the status changes of those ports through alarm information.

**Enabling Log/Trap Output for Ports of MSTP Instance**

<table>
<thead>
<tr>
<th>Table 204</th>
<th>Enable log/trap output for ports of MSTP instance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enable log/trap output for the ports of a specified instance</td>
<td><code>stp [ instance instance-id ] portlog</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable log/trap output for the ports of all instances</td>
<td><code>stp portlog all</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Example**

# Enable log/trap output for the ports of instance 1.

```plaintext
<5500> system-view
[5500] stp instance 1 portlog
```

# Enable log/trap output for the ports of all instances.

```plaintext
<5500> system-view
[5500] stp portlog all
```

**Enabling Trap Messages Conforming to 802.1d Standard**

A switch sends trap messages conforming to 802.1d standard to the network management device in the following two cases:

- The switch becomes the root bridge of an instance.
- Network topology changes are detected.

**Configuration procedure**

<table>
<thead>
<tr>
<th>Table 205</th>
<th>Enable trap messages conforming to 802.1d standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
Table 205 Enable trap messages conforming to 802.1d standard

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable trap messages conforming to 802.1d standard in an instance</td>
<td>stp [ instance instance-id ] dot1d-trap [ newroot</td>
<td>topologychange</td>
</tr>
</tbody>
</table>

Configuration example

# Enable a switch to send trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of instance 1.

<5500> system-view
[5500] stp instance 1 dot1d-trap newroot enable

Displaying and Maintaining MSTP

You can verify the above configurations by executing the display commands in any view.

Execute the reset command in user view to clear statistics about MSTP.

Table 206 Display and maintain MSTP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the state and statistics information about spanning trees of the current device</td>
<td>display stp [ instance instance-id ] [ interface interface-list</td>
</tr>
<tr>
<td>Display region configuration</td>
<td>display stp region-configuration</td>
</tr>
<tr>
<td>Display information about the ports that are shut down by STP protection</td>
<td>display stp portdown</td>
</tr>
<tr>
<td>Display information about the ports that are blocked by STP protection</td>
<td>display stp abnormalport</td>
</tr>
<tr>
<td>Display information about the root port of the instance where the switch reside</td>
<td>display stp root</td>
</tr>
<tr>
<td>Clear statistics about MSTP</td>
<td>reset stp [ interface interface-list ]</td>
</tr>
</tbody>
</table>

MSTP Configuration Example

Network requirements

Implement MSTP in the network shown in Figure 78 to enable packets of different VLANs to be forwarded along different MSTIs. The detailed configurations are as follows:

- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along MSTI1, MSTI3, MSTI4, and MSTI0 respectively.

In this network, Switch A and Switch B operate on the convergence layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the convergence layer and VLAN 40 is limited in the access layer. Switch A and Switch B are configured as the root bridges of MSTI1 and MSTI3 respectively. Switch C is configured as the root bridge of MSTI4.
Network diagram

Figure 78  Network diagram for MSTP configuration

The word *permit* shown in Figure 78 means the corresponding link permits packets of specific VLANs.

**Configuration procedure**

1  Configure Switch A

   # Enter MST region view.
   
   `<5500> system-view
   [5500] stp region-configuration
   
   # Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.
   
   [5500-mst-region] region-name example
   [5500-mst-region] instance 1 vlan 10
   [5500-mst-region] instance 3 vlan 30
   [5500-mst-region] instance 4 vlan 40
   [5500-mst-region] revision-level 0
   
   # Activate the settings of the MST region manually.
   
   [5500-mst-region] active region-configuration
   
   # Specify Switch A as the root bridge of MSTI1.
   
   [5500] stp instance 1 root primary

2  Configure Switch B

   # Enter MST region view.
   
   `<5500> system-view
   [5500] stp region-configuration
   
   # Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.
   
   [5500-mst-region] region-name example
   [5500-mst-region] instance 1 vlan 10
   [5500-mst-region] instance 3 vlan 30
   [5500-mst-region] instance 4 vlan 40
   [5500-mst-region] revision-level 0
   
   # Activate the settings of the MST region manually.
   
   [5500-mst-region] active region-configuration
   
   # Specify Switch B as the root bridge of MSTI3.
   
   [5500] stp instance 3 root primary
3 Configure Switch C.

# Enter MST region view.
<5500> system-view
[5500] stp region-configuration

# Configure the MST region.
[5500-mst-region] region-name example
[5500-mst-region] instance 1 vlan 10
[5500-mst-region] instance 3 vlan 30
[5500-mst-region] instance 4 vlan 40
[5500-mst-region] revision-level 0

# Activate the settings of the MST region manually.
[5500-mst-region] active region-configuration

# Specify Switch C as the root bridge of MSTI4.
[5500] stp instance 4 root primary

4 Configure Switch D

# Enter MST region view.
<5500> system-view
[5500] stp region-configuration

# Configure the MST region.
[5500-mst-region] region-name example
[5500-mst-region] instance 1 vlan 10
[5500-mst-region] instance 3 vlan 30
[5500-mst-region] instance 4 vlan 40
[5500-mst-region] revision-level 0

# Activate the settings of the MST region manually.
[5500-mst-region] active region-configuration

---

**Network requirements**

- Switch C and Switch D are the access devices for the service provider network.
- Switch A and Switch B are the access devices for the customer networks.
- Switch C and Switch D are connected to each other through the configured trunk ports of the switches. The VLAN-VPN tunnel function is enabled in system view, thus implementing transparent transmission between the customer networks and the service provider network.
**Network diagram**

*Figure 79* Network diagram for VLAN-VPN tunnel configuration

**Configuration procedure**

1. Configure Switch A
   
   # Enable MSTP.
   `<5500> system-view
   [5500] stp enable
   # Add Ethernet 1/0/1 to VLAN 10.
   [5500] vlan 10
   [5500-Vlan10] port Ethernet 1/0/1

2. Configure Switch B
   
   # Enable MSTP.
   `<5500> system-view
   [5500] stp enable
   # Add Ethernet 1/0/1 to VLAN 10.
   [5500] vlan 10
   [5500-Vlan10] port Ethernet 1/0/1

3. Configure Switch C
   
   # Enable MSTP.
   `<5500> system-view
   [5500] stp enable
   # Enable the VLAN-VPN tunnel function.
   [5500] vlan-vpn tunnel
   # Add Ethernet 1/0/1 to VLAN 10.
   [5500] vlan 10
   [5500-Vlan10] port Ethernet 1/0/1
   [5500-Vlan10] quit
   # Disable STP on Ethernet 1/0/1 and then enable the VLAN VPN function on it.
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] port access vlan 10
[5500-Ethernet1/0/1] vlan-vpn enable
[5500-Ethernet1/0/1] quit

# Configure Ethernet 1/0/2 as a trunk port.
[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port link-type trunk

# Add the trunk port to all VLANs.
[5500-Ethernet1/0/2] port trunk permit vlan all

4 Configure Switch D

# Enable MSTP.
<5500> system-view
[5500] stp enable

# Enable the VLAN-VPN tunnel function.
[5500] vlan-vpn tunnel

# Add Ethernet 1/0/2 to VLAN 10.
[5500] vlan 10
[5500-Vlan10] port Ethernet 1/0/2

# Disable STP on Ethernet 1/0/2 and then enable the VLAN VPN function on it.
[5500] interface Ethernet1/0/2
[5500-Ethernet1/0/2] port access vlan 10
[5500-Ethernet1/0/2] stp disable
[5500-Ethernet1/0/2] quit

# Configure Ethernet 1/0/1 as a trunk port.
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] port link-type trunk

# Add the trunk port to all VLANs.
[5500-Ethernet1/0/1] port trunk permit vlan all
The term router in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

Introduction to IP Route and Routing Table

**IP Route**

Routers are used for route selection on the Internet. As a router receives a packet, it selects an appropriate route (through a network) according to the destination address of the packet and forwards the packet to the next router. The last router on the route is responsible for delivering the packet to the destination host.

**Routing Table Function**

The key for a router to forward packets is the routing table. Each router maintains a routing table. Each entry in this table contains an IP address that represents a host/subnet and specifies which physical port on the router should be used to forward the packets destined for the host/subnet. And the router forwards those packets through this port to the next router or directly to the destination host if the host is on a network directly connected to the router.

Routes in a routing table can be divided into three categories:

- **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.

**Routing entry**

Each routing entry in a routing table contains:

- **Destination**: It identifies the address of the destination host or network of an IP packet.
- **Mask**: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing logical AND between destination address and network mask, you can get the address of the network segment where the destination host or router resides. For example, if the destination address is 129.102.8.10 and the mask is 255.255.0.0, the address of the network segment where the destination host or router resides is 129.102.0.0. A mask consists of some consecutive 1s, represented either in dotted decimal notation or by the number of the consecutive 1s in the mask.
- Interface: It indicates through which interface IP packets should be forwarded to the destination.
- Nexthop: It indicates the next router that IP packets will pass through to reach the destination.
- Preference: There may be multiple routes with different next hops to the same destination. These routes may be discovered by different routing protocols, or be manually configured static routes. The one with the highest preference (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, routes fall into the following categories:

- Subnet route: The destination is a subnet.
- Host route: The destination is a host.

In addition, according to whether the network where the destination resides is directly connected to the router, routes fall into the following categories:

- Direct route: The router is directly connected to the network where the destination resides.
- Indirect route: The router is not directly connected to the network where the destination resides.

In order to avoid an oversized routing table, you can set a default route. All the packets for which the router fails to find a matching entry in the routing table will be forwarded through this default route.

Figure 80 shows a relatively complicated internet environment, the number in each network cloud indicate the network address. Router G is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in Figure 80.
Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. It cannot adapt itself to any network topology change automatically so that you must perform routing configuration again whenever the network topology changes.

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. It is complicated to configure, and it not only imposes higher requirements on the system than static routing, but also occupies a certain amount of network resources.

Dynamic routing protocols can be classified based on the following standards:
**Operational scope**
- Interior Gateway Protocols (IGPs): Work within an autonomous system, typically including RIP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs): Work between autonomous systems. The most popular one is BGP.

> An autonomous system refers to a group of routers that share the same routing policy and work under the same administration.

**Routing algorithm**
- Distance-vector protocols: RIP and BGP. BGP is also considered a path-vector protocol.
- Link-state protocols: OSPF and IS-IS.

The main differences between the above two types of routing algorithms lie in the way routes are discovered and calculated.

**Type of the destination address**
- Unicast routing protocols: RIP, OSPF, BGP, and IS-IS.
- Multicast routing protocols: PIM-SM and PIM-DM.

This chapter focuses on unicast routing protocols. For information on multicast routing protocols, refer to the chapter entitled “Multicast Overview” on page 385.

**Routing Protocols and Routing Priority**

Different routing protocols may find different routes (including static 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 routing 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:

<table>
<thead>
<tr>
<th>Routing approach</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRECT</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>10</td>
</tr>
<tr>
<td>STATIC</td>
<td>60</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF ASE</td>
<td>150</td>
</tr>
<tr>
<td>OSPF NSSA</td>
<td>150</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>255</td>
</tr>
<tr>
<td>BGP</td>
<td>256</td>
</tr>
</tbody>
</table>

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.

**Load Sharing and Route Backup**

**Load sharing**
A given routing protocol may find several routes with the same metric to the same destination, and if this protocol has the highest priority among all the active protocols, these routes will be considered valid and are used to forward packets, thus achieving load sharing.

**Route backup**
You can configure multiple routes to the same destination, expecting the one with the highest priority to be the primary route and all the rest backup routes.

Route backup can help improve network reliability. Automatic switching can happen between the primary route and a backup route.

Under normal circumstances, packets are forwarded through the primary route. When the primary route goes down, the route with the highest priority among the backup routes is selected to forward packets. When the primary route recovers, the route selection process is performed again and the primary route is selected again to forward packets.

**Routing Information Sharing**
As different routing protocols use different algorithms to calculate routes, they may discover different routes. In a large network with multiple routing protocols, it is required for routing protocols to share their routing information. Each routing protocol shares routing information discovered by other routing protocols through a route redistribution mechanism.

**Displaying and Maintaining a Routing Table**
You can view information in a routing table to locate routing problems. Table 208 lists the commands used to display and maintain a routing table. You can use the `display` commands in any view and the `reset` command to in user view to clear the statistics of a routing table.
### Table 208  Display and maintain a routing table

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display brief information about a routing table</td>
<td>display ip routing-table [ { begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display detailed information about a routing table</td>
<td>display ip routing-table verbose</td>
<td></td>
</tr>
<tr>
<td>Display information about routes permitted by a basic ACL</td>
<td>display ip routing-table acl acl-number [ verbose ]</td>
<td></td>
</tr>
<tr>
<td>Display information about routes permitted by a prefix list</td>
<td>display ip routing-table ip-prefix ip-prefix-name [ verbose ]</td>
<td></td>
</tr>
<tr>
<td>Display routes to a specified destination</td>
<td>display ip routing-table ip-address [ mask</td>
<td>mask-length ] [ longer-match ] [ verbose ]</td>
</tr>
<tr>
<td>Display routes to specified destinations</td>
<td>display ip routing-table ip-address1 [ mask1 ] ip-address2 [ mask2</td>
<td>mask-length2 ] [ verbose ]</td>
</tr>
<tr>
<td>Display routes discovered by a routing protocol</td>
<td>display ip routing-table protocol protocol [ inactive</td>
<td>verbose ]</td>
</tr>
<tr>
<td>Display the tree-structured routing table information</td>
<td>display ip routing-table radix</td>
<td></td>
</tr>
<tr>
<td>Display statistics about a routing table</td>
<td>display ip routing-table statistics</td>
<td></td>
</tr>
<tr>
<td>Clear statistics about a routing table</td>
<td>reset ip routing-table statistics protocol [ all</td>
<td>protocol ]</td>
</tr>
</tbody>
</table>
Introduction to Static Route

Static Route
Static routes are special routes. They are manually configured by the administrator. In a relatively simple network, you only need to configure static routes to make routers work normally. Proper configuration and usage of static routes can improve network performance and ensure sufficient bandwidth for important applications.

When the network topology changes, static routes may become unreachable because they cannot adapt themselves to the change automatically, thus resulting in network interruption. In this case, the network administrator needs to modify the configuration of static routes manually.

Static routes are divided into three types:

- **Reachable route**: normal route. If a static route to a destination is of this type, the IP packets destined for this destination will be forwarded to the next hop. It is the most common type of static routes.

- **Unreachable route**: route with the `reject` attribute. If a static route to a destination has the `reject` attribute, all the IP packets destined for this destination will be discarded, and the source hosts will be informed of the unreachability of the destination.

- **Blackhole route**: route with `blackhole` attribute. If a static route destined for a destination has the `blackhole` attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination will be dropped without notifying the source hosts.

The attributes `reject` and `blackhole` are usually used to limit the range of the destinations this router can reach, and help troubleshoot the network.

Default Route
To avoid too large a routing table, you can configure a default route.

When the destination address of a packet fails to match any entry in the routing table,

- If there is default route in the routing table, the default route will be selected to forward the packet.
CHAPTER 28: STATIC ROUTE CONFIGURATION

- If there is no default route, the packet will be discarded and an ICMP Destination Unreachable or Network Unreachable packet will be returned to the source.

A default route can be manually configured or generated by some dynamic routing protocols, such as OSPF and RIP.

Static Route Configuration

Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of related interfaces
- Configuring IP addresses for related interfaces

Configuring a Static Route

Table 209  Configure a static route

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Configure a static route</td>
<td>ip route-static ip-address { mask</td>
<td>mask-length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the system can obtain the route to the subnet directly connected to the router.</td>
</tr>
</tbody>
</table>

- Use the ip route-static command to configure a default route by setting the destination IP address and the mask to 0.0.0.0.
- Avoid configuring the next hop address of a static route to the address of an interface on the local switch.
- Different preferences can be configured to implement flexible route management policies.
- For automatic detection information, refer to “Auto Detect Configuration” on page 219.

Displaying and Maintaining Static Routes

After completing the above configuration, use the display commands in any view to display and verify the static route configuration. Use the delete command in system view to delete all static routes.

Table 210  Display and maintain static routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current configuration information</td>
<td>display current-configuration</td>
<td>Use the display commands in any view.</td>
</tr>
<tr>
<td>Display the brief information of a routing table</td>
<td>display ip routing-table</td>
<td>—</td>
</tr>
<tr>
<td>Display the detailed information of a routing table</td>
<td>display ip routing-table verbose</td>
<td>—</td>
</tr>
<tr>
<td>Display the information of static routes</td>
<td>display ip routing-table protocol static [ inactive</td>
<td>verbose</td>
</tr>
</tbody>
</table>
Network requirements
A small company requires that any two nodes in its office network communicate with each other, and that the network structure be simple and stable. The company hopes that the existing devices that do not support any dynamic routing protocol can be fully utilized.

In this case, static routes can implement communication between any two nodes.

Network diagram
According to the network requirements, the network topology is designed as shown in Figure 81.

Configuration procedure

When only one interface of the device is interconnected with another network segment, you can implement network communication by configuring either a static route or default route.

1 Perform the following configurations on the switch.

# Approach 1: Configure static routes on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

# Approach 2: Configure a static route on Switch A.

```
delete static-routes all
```

Use the `delete` command in system view.
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2

# Approach 1: Configure static routes on Switch B.

<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1

# Approach 2: Configure a static route on Switch B.

<SwitchB> system-view
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1

# Configure static routes on Switch C.

<SwitchC> system-view
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2

Perform the following configurations on the host.

# Set the default gateway address of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

# Set the default gateway address of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

# Set the default gateway address of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts and switches in the figure can communicate with each other.

### Troubleshooting a Static Route

**Symptom:** The switch is not configured with a dynamic routing protocol. Both the physical status and the link layer protocol status of an interface are UP, but IP packets cannot be forwarded on the interface.

**Solution:** Perform the following procedure.

1. Use the `display ip routing-table protocol static` command to view whether the corresponding static route is correctly configured.

2. Use the `display ip routing-table` command to view whether the static route is valid.
RIP CONFIGURATION

The term router in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

RIP Overview
Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks. RIP is not recommended in complicated large networks.

Basic Concepts
RIP
RIP is a distance-vector (D-V) algorithm-based protocol. It uses port 520 to exchange routing information through UDP packets.

RIP uses hop count (also called routing cost) to measure the distance to a destination address. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite; that is, the destination network or host is unreachable. This limitation makes RIP not suitable for large networks.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes discovered by other routing protocols.

RIP routing database
Each 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 network.
- Next hop: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.
- Interface: Outbound interface on this router, through which IP packets should be forwarded to reach the destination.
- 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.

RIP timers
As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: The period update timer defines the interval between routing updates.
Timeout timer: The timeout timer defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.

Garbage-collection timer: 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) based 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 back to the neighbor to prevent routing loops and save the bandwidth.

RIP Startup and Operation
The whole process of RIP startup and operation is as follows:

- Once RIP is enabled on a router, the router broadcasts or multicasts a request packet to its neighbors. Upon receiving the packet, each neighbor running RIP answers a response packet containing its routing table information.

- When this router receives a response packet, it updates its local routing table and sends a triggered update packet to the neighbors. Upon receiving the triggered update packet, the neighbor sends the packet to all its neighbors. After a series of update triggering processes, each router can get and keep the updated routing information.

- By default, RIP sends its routing table to its neighbors every 30 seconds. Upon receiving the packets, the neighbors maintain their own routing tables and select optimal routes, and then advertise update information to their respective neighbors so as to make the updated routes known globally. Furthermore, RIP uses the aging mechanism to handle the timeout routes to ensure real-time and valid routes.

RIP Configuration Tasks

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic RIP functions</td>
<td>Required</td>
</tr>
<tr>
<td>Enabling RIP</td>
<td></td>
</tr>
<tr>
<td>Setting the RIP operating status on an interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Specifying a RIP version</td>
<td></td>
</tr>
</tbody>
</table>
Basic RIP Configuration

### Prerequisites

Before configuring basic RIP functions, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer

### Enabling RIP on the interfaces attached to a specified network segment

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enable RIP and enter RIP view</td>
<td>rip</td>
<td>Required</td>
</tr>
<tr>
<td>Enable RIP on the specified interface</td>
<td>network network-address</td>
<td>Required</td>
</tr>
</tbody>
</table>

- Related RIP commands configured in interface view can take effect only after RIP is enabled.

- RIP operates on the interfaces attached to a specified network segment. When RIP is disabled on an interface, it does not operate on the interface, that is, it neither receives/sends routes on the interface, nor forwards its any interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.
Setting the RIP operating status on an interface

Table 213  Set the RIP operating status on an interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Enable the interface to receive RIP update packets</td>
<td>rip input</td>
<td>Optional</td>
</tr>
<tr>
<td>Enable the interface to send RIP update packets</td>
<td>rip output</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Enable the interface to receive and send RIP update packets</td>
<td>rip work</td>
<td>—</td>
</tr>
</tbody>
</table>

Specifying the RIP version on an interface

Follow the instructions in Table 214 to specify the RIP version on an interface.

Table 214  Specify the RIP version on an interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Specify the version of the RIP running on the interface</td>
<td>rip version { 1</td>
<td>2 [ broadcast</td>
</tr>
</tbody>
</table>

By default, the version of the RIP running on an interface is RIP-1.

RIP Route Control

In actual implementation, it may be needed to control RIP routing information more accurately to accommodate complex network environments. By performing the configuration described in the following sections, you can:

- Control route selection by adjusting additional routing metrics on interfaces running RIP.
- Reduce the size of the routing table by setting route summarization and disabling the receiving of host routes.
- Filter incoming and outgoing routes.
- Set the preference of RIP to change the preference order of routing protocols. This order makes sense when more than one route to the same destination is discovered by multiple routing protocols.
- Redistribute external routes in an environment with multiple routing protocols.

**Configuration Prerequisites**

Before configuring RIP route control, perform the following tasks:

- Configuring network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

**Configuring RIP Route Control**

Setting the additional routing metrics of an interface

Additional metric is the metric added to the original metrics of RIP routes on an interface. It does not directly change the metric value of a RIP route in the routing
table of a router, but will be added to incoming or outgoing RIP routes on the interface.

Table 215  Set additional routing metric

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Set the additional routing metric to be added</td>
<td>rip metricin value</td>
<td>Optional</td>
</tr>
<tr>
<td>for incoming RIP routes on this interface</td>
<td></td>
<td>0 by default</td>
</tr>
<tr>
<td>Set the additional routing metric to be added</td>
<td>rip metricout value</td>
<td>Optional</td>
</tr>
<tr>
<td>for outgoing RIP routes on this interface</td>
<td></td>
<td>1 by default</td>
</tr>
</tbody>
</table>

The rip metricout command takes effect only on the RIP routes learnt by the router and the RIP routes generated by the router itself, but the command is invalid for any route imported to RIP from other routing protocols.

Configuring RIP route summarization

Rip route summarization means that when the router advertises RIP updates, different subnet routes in the same natural network segment can be aggregated into one route with a natural mask for transmission to another network segment. This function is used to reduce the routing traffic on the network as well as the size of the routing table.

When it is necessary to advertise RIP route updates in a subnet, disable the route summarization for RIP-2.

Table 216  Configure RIP route summarization

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
<td>—</td>
</tr>
<tr>
<td>Enable RIP-2 automatic route summarization</td>
<td>summary</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, RIP-2 automatic route summarization is enabled.</td>
</tr>
</tbody>
</table>

Disabling the router from receiving host routes

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After a router is disabled from receiving host routes, it can refuse any incoming host route.

Table 217  Disable the router from receiving host routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
<td>—</td>
</tr>
</tbody>
</table>
CHAPTER 29: RIP CONFIGURATION

Configuring RIP to filter incoming/outgoing routes

The route filtering function provided by a router enables you to configure inbound/outbound filter policy by specifying an ACL, address prefix list, or routing policy to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Table 217 Disable the router from receiving host routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the router from receiving host routes</td>
<td>undo host-route</td>
<td>Required By default, the router receives host routes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
<td>—</td>
</tr>
<tr>
<td>Configure RIP to filter incoming routes</td>
<td>filter-policy {</td>
<td>Required By default, RIP does not filter any incoming route.</td>
</tr>
<tr>
<td></td>
<td>acl-number</td>
<td>gateway ip-prefix-name</td>
</tr>
<tr>
<td>Configure RIP to filter outgoing routes</td>
<td>filter-policy gateway ip-prefix-name import</td>
<td>Required By default, RIP does not filter any outgoing route.</td>
</tr>
<tr>
<td></td>
<td>filter-policy { acl-number</td>
<td>ip-prefix-name</td>
</tr>
</tbody>
</table>

- The **filter-policy import** command filters the RIP routes received from neighbors, and the routes being filtered out will neither be added to the routing table nor be advertised to any neighbors.

- The **filter-policy export** command filters all the routes to be advertised, including the routes redistributed with the **import-route** command and routes learned from neighbors.

- You can also use the **filter-policy export** command to filter outgoing routes redistributed from a specified routing protocol.

Setting RIP preference

Table 219 Set RIP preference

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
<td>—</td>
</tr>
<tr>
<td>Set the RIP preference</td>
<td>preference value</td>
<td>Required</td>
</tr>
</tbody>
</table>

The default RIP preference is 100.
Enabling load sharing among RIP interfaces

Table 220 Enable load sharing among RIP interfaces

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view -</td>
<td></td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip -</td>
<td></td>
</tr>
<tr>
<td>Enable load sharing among RIP interfaces</td>
<td>traffic-share-across-interface face</td>
<td>Required By default, load sharing among RIP interfaces is disabled</td>
</tr>
</tbody>
</table>

Configuring RIP to redistribute routes from another protocol

Table 221 Configure RIP to import routes from another protocol

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view -</td>
<td></td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip -</td>
<td></td>
</tr>
<tr>
<td>Configure a default cost for an incoming route</td>
<td>default cost value Optional 1 by default.</td>
<td></td>
</tr>
<tr>
<td>Configure RIP to redistribute routes from another protocol</td>
<td>import-route protocol { process-id</td>
<td>allow-ibgp } [ cost value</td>
</tr>
</tbody>
</table>

In some special network environments, some RIP features need to be configured and RIP network performance needs to be adjusted and optimized. By performing the configuration mentioned in this section, the following can be implemented:

- Changing the convergence speed of RIP network by adjusting RIP timers,
- Avoiding routing loops by configuring split horizon,
- Packet validation in network environments with high security requirements, and
- Configuring RIP to unicast RIP messages on an interfaces with special requirements.

Configuration Prerequisites

Before adjusting RIP, perform the following tasks:

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuration Tasks

Configuring RIP timers

Table 222 Configure RIP timers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view -</td>
<td></td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip -</td>
<td></td>
</tr>
<tr>
<td>Set the RIP timers</td>
<td>timers { update update-timer</td>
<td>timeout timeout-timer } * Required By default, the Update timer is 30 seconds and the Timeout timer 180 seconds.</td>
</tr>
</tbody>
</table>
When configuring the values of RIP timers, you should take network performance into consideration and perform consistent configuration on all routers running RIP to avoid unnecessary network traffic and network route oscillation.

**Configuring split horizon**

<table>
<thead>
<tr>
<th>Table 223</th>
<th>Configure split horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Enable split horizon</td>
<td>rip split-horizon</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Split horizon cannot be disabled on a point-to-point link.*

**Configuring RIP-1 packet zero field check**

<table>
<thead>
<tr>
<th>Table 224</th>
<th>Configure RIP-1 packet zero field check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
</tr>
<tr>
<td>Enable the check of the must be zero field in RIP-1 packets</td>
<td>checkzero</td>
</tr>
</tbody>
</table>

*Some fields in a RIP-1 packet must be 0, and they are known as must be zero field. For RIP-1, the must be zero field is checked for incoming packets, and those RIP-1 packets with this field being nonzero will not be processed.*

**Setting RIP-2 packet authentication mode**

RIP-2 supports two authentication modes: simple authentication and message digest 5 (MD5) authentication.

Simple authentication cannot provide complete security, because the authentication keys sent along with packets that are not encrypted. Therefore, simple authentication cannot be applied where high security is required.

<table>
<thead>
<tr>
<th>Table 225</th>
<th>Set RIP-2 packet authentication mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Set RIP-2 packet authentication mode</td>
<td>rip authentication-mode (simple password</td>
</tr>
</tbody>
</table>

If you specify to use MD5 authentication, you must specify one of the following MD5 authentication types:

- rfc2453 (this type supports the packet format defined in RFC 2453)
- rfc2082 (this type supports the packet format defined in RFC 2082)
Configuring RIP to unicast RIP packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter RIP view</td>
<td>rip</td>
<td></td>
</tr>
<tr>
<td>Configure RIP to</td>
<td>peer ip-address</td>
<td>Required</td>
</tr>
<tr>
<td>unicast RIP packets</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When RIP runs on the link that does not support broadcast or multicast, you must configure RIP to unicast RIP packets.

Displaying and Maintaining RIP Configuration

After completing the above configuration, you can use the display command to display the running status of RIP and verify the RIP configuration. You can use the reset command to reset the system configuration related to RIP.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current RIP running status and configuration information</td>
<td>display rip</td>
<td>You can execute the display command in any view.</td>
</tr>
<tr>
<td>Display RIP interface information</td>
<td>display rip interface</td>
<td></td>
</tr>
<tr>
<td>Display RIP routing information</td>
<td>display rip routing</td>
<td></td>
</tr>
<tr>
<td>Reset the system configuration related to RIP</td>
<td>reset</td>
<td>You can use this command in RIP view.</td>
</tr>
</tbody>
</table>

RIP Configuration Example

Network requirements

A small-sized company requires that any two nodes in its small office network communicate with each other, and that the network devices automatically adapt themselves to any topology change so as to reduce the work of manual maintenance.

In this case, RIP can implement communication between any two nodes.

Network diagram

According to the network requirements, the network topology is designed as shown in Figure 82.

Figure 82  Network diagram for RIP configuration
CHAPTER 29: RIP CONFIGURATION

Configuration procedure

Only the configuration related to RIP is listed below. Before the following configuration, make sure the Ethernet link layer works normally and the IP addresses of VLAN interfaces are configured correctly.

1 Configure Switch A:

# Configure RIP.

<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0

2 Configure Switch B:

# Configure RIP.

<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0

3 Configure Switch C:

# Configure RIP.

<SwitchC> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0

Troubleshooting RIP Configuration

Failed to Receive RIP Updates

Symptom
The Ethernet switch cannot receive any RIP update when the physical connection between the switch and the peer routing device is normal.

Solution
Check that:

- RIP is enabled by using the network command on the corresponding interface.
- The interface is allowed to receive or send RIP packets.
■ The interface receives RIP packets in the way the peer device sends them, for example, in the broadcast or multicast mode.
The term router in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

OSPF Overview

Introduction to OSPF
Open Shortest Path First (OSPF) is a link state-based interior gateway protocol developed by IETF. At present, OSPF version 2 (RFC 2328) is used, which has the following features:

- High applicability: OSPF supports various networks in size, and even networks with up to several hundred routers.
- Fast convergence: OSPF can transmit update packets immediately after the network topology changes so that the change can be synchronized in the autonomous system (AS).
- Loop-free: Since OSPF calculates routes with the shortest path first algorithm according to the collected link states, it guarantees that no loop routes will be generated.
- Area partition: OSPF allows an autonomous system network to be divided into different areas for convenient management so that routing information transmitted between the areas is summarized further, thereby reducing network bandwidth consumption.
- Equivalent route: OSPF supports multiple equivalent routes to the same destination.
- Routing hierarchy: OSPF has a four-level routing hierarchy. It prioritizes the routes as intra-area, inter-area, external type-1, and external type-2 routes.
- Authentication: OSPF supports interface-based packet authentication to guarantee the security of route calculation.
- Multicast transmission: OSPF supports transmitting protocol packets in multicast mode.

OSPF Route Calculation
Taking no account of area partition, the routing calculation process of the OSPF protocol is as follows:

- Each OSPF-supported router maintains a link state database (LSDB), which describes the topology of the whole AS. According to the network topology around itself, each router generates a link state advertisement (LSA). Routers on the network exchange LSAs with each other by transmitting protocol packets. Thus, each router receives the LSAs of other routers and all these LSAs form the LSDB of the router.
An LSA describes the network topology around a router, whereas an LSDB describes the network topology of the whole network. Routers can transform the LSDB to a weighted, directed graph, which reflects the real topology of the whole network. All routers get exactly the same weighted, directed graph.

According to the weighted, directed graph, each router uses the shortest path first (SPF) algorithm to calculate the shortest path tree with itself as the root. The tree shows the routes to the nodes in the autonomous system. External routes are leaf nodes, which are marked with the routers from which they are advertised to record information outside the AS. The routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast their local status information (such as available interface information and reachable neighbor information) to the whole AS, routers in the AS should establish adjacencies among them. In this case, the route changes on any router will result in multiple transmissions, which are unnecessary and waste the precious bandwidth resources. To solve this problem, designated router (DR) and backup designated router (BDR) are defined in OSPF. For details about DR and BDR, see “DR/BDR introduction” on page 309.

OSPF supports interface-based packet authentication to guarantee the security of route calculation. In addition, it transmits and receives packets in multicast (224.0.0.5 and 224.0.0.6).

### Basic OSPF Concepts

#### Autonomous System
A set of routers using the same routing protocol to exchange routing information constitute an Autonomous System (AS).

#### Router ID
To run OSPF, a router must have a router ID. A router ID can be configured manually. If no router ID is configured, the system will automatically select an IP address from the IP addresses of the interfaces as the router ID. A router ID is selected in the following way:

- If loopback interface addresses are configured, the system chooses the latest configured loopback interface IP address as the router ID.
- If no loopback interface is configured, the first configured IP address among the IP addresses of other interfaces will be the router ID.

#### OSPF Packets
OSPF uses five types of packets:

- **Hello packet:**
  
  Hello packets are most commonly used OSPF packets, which are periodically sent by a router to its neighbors. A Hello packet contains the values of some timers, DR, BDR and known neighbors.

- **DD packet:**
  
  When two routers synchronize their databases, they use database description (DD) packets to describe their own LSDBs, including the summary of each LSA. The summary refers to the header of an LSA which uniquely identifies the LSA. This
reduces the size of traffic transmitted between the routers because the header of an LSA only occupies a small portion of the LSA. With the header, the peer router can judge whether it has the LSA or not.

- **LSR packet:**

After exchanging DD packets, the two routers know which LSAs of the peer router are lacked in the local LSDB, and send link state request (LSR) packets requesting for the lacked LSAs to the peer. These LSR packets contain the digest of the needed LSAs.

- **LSU packet:**

Link state update (LSU) packets are used to transmit the needed LSAs to the peer router. An LSU packet is a collection of multiple LSAs (complete LSAs, not LSA digest).

- **LSAck packet**

Link state acknowledgment (LSAck) packets are used to acknowledge received LSU packets. An LSAck contains the header(s) of LSA(s) to be acknowledged (One LSAck packet can acknowledge multiple LSAs).

**LSA Types**

1. **Five basic LSA types**

As described in the preceding sections, LSAs are the primary source for OSPF to calculate and maintain routes. RFC 2328 defines five types of LSAs:

- **Router-LSA:** Type-1 LSAs, generated by every router to describe the router’s link states and costs, and advertised only in the originating area.

- **Network-LSA:** Type-2 LSAs, generated by the DRs on a broadcast or NBMA network to describe the link states of the current network segment, and are advertised only in the originating area.

- **Summary-LSA:** Type-3 and Type-4 LSAs, generated by ABRs and advertised in the areas associated with the LSAs. Each Summary-LSA describes a route to a destination in another area of the AS (also called inter-area route). Type-3 Summary-LSAs are for routes to networks (that is, their destinations are segments), while Type-4 Summary-LSAs are for routes to ASBRs.

- **AS-external-LSA:** Type-5 LSA, also called ASE LSA, generated by ASBRs to describe the routes to other ASs and advertised to the whole AS (excluding stub areas and NSSA areas). The default AS route can also be described by AS-external-LSAs.

2. **Type-7 LSAs**

In RFC 1587 (OSPF NSSA Option), Type-7 LSA, a new LSA type, is added.

As described in RFC 1587, Type-7 LSAs and Type-5 LSAs mainly differ in the following two ways:

- **Type-7 LSAs** are generated and advertised in an NSSA, where Type-5 LSAs will not be generated or advertised.
Type-7 LSAs can only be advertised in an NSSA area. When Type-7 LSAs reach an ABR, the ABR can convert part of the routing information carried in the Type-7 LSAs into Type-5 LSAs and advertise the Type-5 LSAs. Type-7 LSAs are not directly advertised to other areas (including the backbone area).

Neighbor and Adjacency

In OSPF, the Neighbor and Adjacency are two different concepts.

Neighbor: Two routers that have interfaces to a common network. Neighbor relationships are maintained by, and usually dynamically discovered by, OSPF’s hello packets. When a router starts, it sends a hello packet through the OSPF interface, and the router that receives the hello packet checks parameters carried in the packet. If parameters of the two routers match, they become neighbors.

Adjacency: A relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers become adjacent, which depends on network types. Only by synchronizing the LSDB by exchanging DD packets and LSAs can two routers become adjacent.

OSPF Area Partition and Route Summarization

Area partition

If all the routers on an ever-growing large network run OSPF, the large number of routers will result in an enormous LSDB, which will consume an enormous storage space, complicate the running of SPF algorithm, and increase CPU load.

Furthermore, as a network grows larger, it is more likely to have changes in the network topology. Hence, the network will often be flapping, and a great number of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utilization. Even worse, any change of the topology will cause all the routers on the network to re-perform route calculation.

OSPF solves the above-mentioned problem by dividing an AS into multiple areas. Areas refer to groups into which routers are logically divided. Each group is identified by an Area ID, as shown in Figure 83.
Figure 83  OSPF area partition

On the border of an area is a router, which belongs to different areas. After area partition, area border routers perform route summarization to reduce the number of LSAs advertised to other areas and minimize the effect of topology changes.

**Classification of routers**

The OSPF router falls into four types according to the position in the AS:

1. **Internal router**

   All interfaces on an internal router belong to one OSPF area.

2. **Area border router (ABR)**

   An area border router belongs to more than two areas, one of which must be the backbone area. It connects the backbone area to a non-backbone area. The connection between an area border router and the backbone area can be physical or logical.

3. **Backbone router**

   At least one interface of a backbone router must be attached to the backbone area. Therefore, all ABRs and internal routers in area 0 are backbone routers.

4. ** Autonomous system border router (ASBR)**

   The router exchanging routing information with another AS is an ASBR, which may not reside on the boundary of the AS. It can be an internal router or area border router.

5. ** Type-7 LSAs translator**
A Type-7 LSAs translator takes effect on an ABR. The state of the Type-7 LSAs translator determines whether the ABR needs to translate Type-7 LSAs into Type-5 LSAs.

- When the Type-7 LSAs translator state is **Enabled** or **Elected**, the ABR translates Type-7 LSAs into Type-5 LSAs.
- When the Type-7 LSAs translator state is **Disabled**, the ABR does not translate Type-7 LSAs into Type-5 LSAs.

**Figure 84** OSPF router types

Backbone area and virtual link

1 Backbone area

With OSPF area partition, not all areas are equal. One of the areas is different from any other area. Its area ID is 0 and it is usually called the backbone area. Routing information between non-backbone areas must be forwarded by the backbone area. Therefore, OSPF requires:

- All non-backbone areas must maintain connectivity to the backbone area.
- The backbone area itself must maintain connectivity.

In practice, due to physical limitations, the requirements may not be satisfied. In this case, configuring OSPF virtual links is a solution.

2 Virtual link
A virtual link is established between two area border routers through a non-backbone area and is configured on both ABRs to take effect. The area that provides the non-backbone area internal route for the virtual link is a **transit area**.

In the following figure, Area 2 has no direct physical link to the backbone area 0. Configuring a virtual link between ABRs can connect Area 2 to the backbone area.

**Figure 85** Virtual link application 1

![Virtual link application 1](image)

Another application of virtual links is to provide redundant links. If the backbone area cannot maintain internal connectivity due to a physical link failure, configuring a virtual link can guarantee logical connectivity in the backbone area, as shown below.

**Figure 86** Virtual link application 2

![Virtual link application 2](image)

The virtual link between the two ABRs acts as a point-to-point connection. Therefore, you can configure interface parameters such as hello packet interval on the virtual link as they are configured on physical interfaces.

The two ABRs on the virtual link exchange OSPF packets with each other directly, the OSPF routers in between simply convey these OSPF packets as normal IP packets.

**(Totally) Stub area**

The ABR in a stub area does not distribute Type-5 LSAs into the area, so the routing table scale and amount of routing information in this area are reduced significantly.

You can also configure the stub area as a Totally Stub area, where the ABR advertises neither the routes of other areas nor the external routes.

Stub area configuration is optional, and not every area is qualified to be a stub area. In general, a stub area resides on the border of the AS.
The ABR in a stub area generates a default route into the area.

Note the following when configuring a (totally) stub area:

- The backbone area cannot be a (totally) stub area
- The stub command must be configured on routers in a (totally) stub area
- A (totally) stub area cannot have an ASBR because AS external routes cannot be distributed into the stub area.
- Virtual links cannot transit (totally) stub areas.

NSSA area

Similar to a stub area, an NSSA area imports no AS external LSA (Type-5 LSA) but can import Type-7 LSAs that are generated by the ASBR and distributed throughout the NSSA area. When reaching the NSSA ABR, Type-7 LSAs are translated into Type-5 LSAs by the ABR (the Type-7 LSAs translator state must be enabled/elected) before being advertised to other areas.

In Figure 87, the OSPF AS contains three areas: Area 1, Area 2 and Area 0. The other two ASs employ the RIP protocol. Area 1 is an NSSA area, and the ASBR in it translates RIP routes into Type-7 LSAs and advertises them throughout Area 1. When these LSAs reach the NSSA ABR with the Type-7 LSAs translator state as Enabled or Elected, the ABR translates Type-7 LSAs to Type-5 LSAs for advertisement to Area 0 and Area 2.

On the left of the figure, RIP routes are translated into Type-5 LSAs by the ASBR of Area 2 and distributed into the OSPF AS. However, Area 1 is an NSSA area, so these Type-5 LSAs cannot travel to Area 1.

Similar to stub areas, virtual links cannot transit NSSA areas.

Figure 87  NSSA area

Route summarization

Route summarization: An ABR or ASBR summarizes routes with the same prefix with a single route and distribute it to other areas.

After an AS is divided into different areas that are interconnected through OSPF ABRs, The routing information between areas can be reduced through route summarization. This reduces the size of routing tables and improves the calculation speed of routers.

After an ABR in an area calculates the intra-area routes in the area, the ABR aggregates multiple OSPF routes into one LSA (based on the summarization configuration) and sends the LSA outside the area.
For example, as shown in the following figure, in Area 1 are three internal routes 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. By configuring route summarization on Router A, the three routes are summarized with the route 19.1.0.0/16 that is advertised into Area 0.

Figure 88 Route summarization

OSPF has two types of route summarization:

1. ABR route summarization

To distribute routing information to other areas, an ABR generates Type-3 LSAs on a per network segment basis for an attached non-backbone area. If contiguous network segments are available in the area, you can summarize them with a single network segment. The ABR in the area distributes only the summary LSA to reduce the scale of LSDBs on routers in other areas.

2. ASBR route summarization

If summarization for redistributed routes is configured on an ASBR, it will summarize redistributed Type-5 LSAs that fall into the specified address range. If in an NSSA area, it also summarizes Type-7 LSAs that fall into the specified address range.

If this feature is configured on an ABR, the ABR will summarize Type-5 LSAs translated from Type-7 LSAs.

Route types

OSPF prioritizes routes according to four levels:

- Intra-area route
- Inter-area route
- type1 external route
- type2 external route

The intra-area and inter-area routes describe the network topology of the AS, while external routes describe routes to destinations outside the AS. OSPF classifies external routes into two types: type1 and type2.

A type1 external route is an IGP route, such as a RIP or static route, which has high credibility and whose cost is comparable with the cost of an OSPF internal route. The cost from a router to the destination of the type1 external route = the cost from the router to the corresponding ASBR + the cost from the ASBR to the destination of the external route.

A type2 external route is an EGP route, which has low credibility, so OSPF considers the cost from the ASBR to the destination of the type2 external route is
much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from the internal router to the destination of the type2 external route= the cost from the ASBR to the destination of the type2 external route. If two routes to the same destination have the same cost, then take the cost from the router to the ASBR into consideration.

**OSPF Network Type**

**Four OSPF network types**

OSPF divides networks into four types by link layer protocols:

- **Broadcast**: If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast. In a broadcast network, protocol packets are sent in multicast (224.0.0.5 and 224.0.0.6) by default.

- **Non-broadcast multi-access (NBMA)**: If Frame Relay, ATM, or X.25 is adopted, OSPF defaults the network type to NBMA. In an NBMA network, protocol packets are sent in unicast.

- **Point-to-multipoint (P2MP)**: OSPF will not default the network type of any link layer protocol to P2MP. A P2MP network must be compulsorily changed from another network type. The common practice is to change an NBMA network into a P2MP network. In a P2MP network, protocol packets are sent to the multicast address (224.0.0.5) by default, but protocol packets can be sent in the unicast address as needed.

- **Point-to-point (P2P)**: If PPP or HDLC is adopted, OSPF defaults the network type to P2P. In a P2P network, protocol packets are sent in multicast (224.0.0.5).

**Principles for configuring an NBMA network**

An NBMA network is a non-broadcast and multi-accessible network. ATM and frame relay networks are typical NBMA networks.

Some special configurations need to be done on an NBMA network. In an NBMA network, an OSPF router cannot discover an adjacent router by broadcasting Hello packets. Therefore, you must manually specify an IP address for the adjacent router and whether the adjacent router has the right to vote for a DR.

An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit. If two routers in the network are not directly reachable to each other, you must configure the corresponding interface type to P2MP. If a router in the network has only one neighbor, you can change the corresponding interface type to P2P.

The differences between NBMA and P2MP are as follows:

- An NBMA network is fully connected, non-broadcast, and multi-accessible, whereas a P2MP network is not necessarily fully connected.

- DR and BDR are required to be elected on an NBMA network but not on a P2MP network.

- NBMA is a default network type. A P2MP network, however, must be compulsorily changed from another network type. The more common practice is to change an NBMA network into a P2MP network.

- Since NBMA interfaces send packets to unicast addresses, you need to configure neighbors manually. By default, P2MP sends protocol packets to multicast addresses.
**DR/BDR introduction**

In a broadcast network or an NBMA network, routing information needs to be transmitted between any two routers. If there are \( n \) routers in the network, \( n \times \frac{(n-1)}{2} \) adjacencies need to be established. In this case, the route changes on any router will result in multiple transmissions, which waste bandwidth. To solve this problem, DR is defined in OSPF so that all routers send information to the DR only and the DR broadcasts the network link states in the network.

If the DR fails, a new DR must be elected and synchronized with the other routers on the network. The process takes quite a long time; in the process, route calculation is incorrect. To shorten the process, BDR is introduced in OSPF.

A BDR provides backup for a DR. DR and BDR are elected at the same time. Adjacencies are also established between the BDR and all the other routers on the segment, and routing information is also exchanged between them. Once the DR becomes invalid, the BDR becomes a DR. Since no re-election is needed and the adjacencies already exist, the switchover process is very short. Now, a new BDR should be elected. Although this election process will also take quite a long time, route calculation will not be affected.

On an OSPF network, a router which is neither DR nor BDR is called DR Other. It establishes adjacencies with the DR and BDR, but not with other DR Others. This reduces not only the number of adjacencies among routers, but also the network traffic and occupied bandwidth resources on the broadcast or NBMA network.

In Figure 89, the solid lines represent physical Ethernet connections and the dotted lines represent adjacencies established. The figure shows that, with the DR/BDR mechanism adopted, seven adjacencies suffice among the five routers.

**Figure 89** DR/BDR

**DR/BDR election**

The DR and BDR in a network are elected by all routers rather than configured manually. The DR priority of an interface determines its qualification for DR/BDR election. Interfaces attached to the network and having priorities higher than 0 are election candidates.

The election votes are hello packets. Each router sends the DR elected by itself in a hello packet to all the other routers. If two routers on the network declare themselves as the DR, the router with the higher DR priority wins. If DR priorities are the same, the router with the higher Router ID wins. In addition, a router with the priority 0 cannot become the DR/BDR.
Note the following points:

- DR election is required for broadcast or NBMA interfaces but is not required for P2P or P2MP interfaces.
- DR is based on the router interfaces in a certain segment. A router may be a DR on an interface and a BDR or DR Other on another interface.
- The priority of a router affects the DR and BDR election. However, it has no effect on the election after the DR and BDR election ends. A new priority assigned to the router takes effect at the time of next DR and BDR election.
- If a new router is added after DR and BDR election, the router does not become the DR immediately even if it has the highest DR priority.
- The DR on a network segment is unnecessarily the router with the highest priority. Likewise, the BDR is unnecessarily the router with the second highest priority.

**OSPF Features**

The Switch 5500 supports the following OSPF features:

- Stub area: Stub area is defined to reduce the cost for the routers in the area to receive ASE routes.
- NSSA: NSSA is defined to remove the limit on the topology in a Stub area.
- OSPF multi-process: Multiple OSPF processes can be run on a router.
- Sharing discovered routing information with other dynamic routing protocols: At present, OSPF supports importing the routes of other dynamic routing protocols (such as RIP), and static routes as OSPF external routes into the AS to which the router belongs. In addition, OSPF supports advertising the routing information it discovered to other routing protocols.
- Packet authentication: OSPF supports the authentication of the packets between neighboring routers in the same area by using one of the two methods: plain text authentication and MD5 authentication.
- Flexible configuration of router interface parameters: For a router interface, you can configure the following OSPF parameters: output cost, Hello interval, retransmission interval, interface transmission delay, route priority, dead time for a neighboring router, and packet authentication mode and authentication key.
- Virtual link: Virtual links can be configured.

**OSPF Configuration Tasks**

**Table 228  OSPF configuration tasks**

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic OSPF configuration</td>
<td>Required</td>
</tr>
<tr>
<td>OSPF area attribute configuration</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Before you can configure other OSPF features, you must first enable OSPF and specify the interface and area ID.

### Configuration Prerequisites

Before configuring OSPF, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF network type configuration</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the network type of an OSPF interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring an NBMA/P2MP neighbor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the DR priority on an OSPF interface</td>
<td>Optional</td>
</tr>
<tr>
<td>OSPF route control</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF route summarization</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF to filter received routes</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF interface cost</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF route priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the maximum number of OSPF ECMP routes</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF to redistribute external routes</td>
<td>Optional</td>
</tr>
<tr>
<td>OSPF network adjustment and optimization</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF timers</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the LSA transmission delay</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the SPF calculation interval</td>
<td>Optional</td>
</tr>
<tr>
<td>Disabling OSPF packet transmission on an interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF authentication</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the MTU field in DD packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling OSPF logging of neighbor state changes</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring OSPF network management</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Table 228  OSPF configuration tasks

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF network type configuration</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the network type of an OSPF interface</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring an NBMA/P2MP neighbor</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the DR priority on an OSPF interface</td>
<td>Optional</td>
</tr>
</tbody>
</table>

---

*Basic OSPF Configuration*
Basic OSPF Configuration

Basic OSPF configuration includes:

- **Configuring router ID**

To ensure stable OSPF operation, you should determine the division of router IDs and manually configure them when implementing network planning. When you configure router IDs manually, make sure each router ID is uniquely used by one router in the AS. A common practice is to set the IP address of an interface on the router to the router ID.

- **Enabling OSPF**

The 3600 Series Ethernet Switches support multiple OSPF processes. To enable multiple OSPF processes on a router, you need to specify different process IDs. OSPF process ID is only locally significant; it does not affect the packet exchange between an OSPF process and other routers. Therefore, packets can be exchanged between routers with different OSPF processes IDs.

- **Configuring an area and the network segments in the area.** You need to plan areas in an AS before performing the corresponding configurations on each router.

When configuring the routers in the same area, please note that most configurations should be uniformly made based on the area. Wrong configuration may disable information transmission between neighboring routers and even lead to congestion or self-loop of routing information.

<table>
<thead>
<tr>
<th>Table 229</th>
<th>Basic OSPF configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Configure the router ID</td>
<td>router id router-id</td>
</tr>
<tr>
<td>Enable OSPF and enter OSPF view</td>
<td>ospf [ process-id [ router-id router-id ] ]</td>
</tr>
<tr>
<td>Enter OSPF area view</td>
<td>area area-id</td>
</tr>
<tr>
<td>Configure the network segments in the area</td>
<td>network ip-address wildcard-mask</td>
</tr>
</tbody>
</table>

- In router ID selection, the priorities of the router IDs configured with the `ospf [ process-id [ router-id router-id ] ]` command, the `router id` command, and the priorities of the router IDs automatically selected are in a descending order.

- **Router IDs can be re-selected.** A re-selected router ID takes effect only after the OSPF process is restarted.

- The `ospf [ process-id [ router-id router-id ] ]` command is recommended for configuring router IDs manually.

- An OSPF process ID on a router must be unique.
One segment can belong to only one area and you must specify each OSPF interface to belong to a particular area.

**OSPF Area Attribute Configuration**

Area partition in OSPF reduces the number of LSAs in the network and enhances OSPF scalability. To further reduce routing table size and the number of LSAs in some non-backbone areas on the edge of the AS, you can configure these areas as stub areas.

A stub area cannot redistribute any external route. For this reason the concept of NSSA is introduced. Type7 LSAs can be advertised in an NSSA. Type7 LSAs are generated by ASBRs in the NSSA, and will be transformed into Type5 LSAs (AS-external LSAs) when reaching ABRs in the NSSA area, which will then be advertised to other areas.

After area partition, the OSPF route updates between non-backbone areas are exchanged by way of the backbone area. Therefore, OSPF requires that all the non-backbone areas should keep connectivity with the backbone area and the backbone area must keep connectivity in itself.

If the physical connectivity cannot be ensured due to various restrictions, you can configure OSPF virtual links to satisfy this requirement.

**Configuration Prerequisites**

Before configuring OSPF area attributes, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Performing basic OSPF configuration

**Configuring OSPF Area Attributes**

<table>
<thead>
<tr>
<th>Table 230 Configure OSPF area attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Enter OSPF view</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Enter OSPF area view</td>
</tr>
</tbody>
</table>
| Configure the current area to be a stub area | stub [ no-summary ] | Optional
| By default, no area is configured as a stub area. |
| Configure the current area to be an NSSA area | nssa [ default-route-advertise | Optional
| By default, no area is configured as an NSSA area. |
| | no-import-route | |
| | no-summary | |
| | translate-always ]* | |
| Configure the cost of the default route transmitted by OSPF to a stub or NSSA area | default-cost cost | Optional
| This can be configured on an ABR only. By default, the cost of the default route to a stub or NSSA area is 1. |
You must use the **stub** command on all the routers connected to a stub area to configure the area with the stub attribute.

You must use the **nssa** command on all the routers connected to an NSSA area to configure the area with the NSSA attribute.

**OSPF Network Type Configuration**

OSPF divides networks into four types by link layer protocol. See “OSPF Network Type” on page 308. An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit. However, in many cases, this cannot be implemented and you need to use a command to change the network type forcibly.

Configure the network type of an interface as P2MP if not all the routers are directly accessible on an NBMA network. You can also configure the network type of an interface to P2P if the router has only one peer on the NBMA network.

In addition, when configuring a broadcast network or NBMA network, you can also specify DR election priority for each interface of a router to control the DR/BDR election in the network. Thus, the router with higher performance and reliability can be selected as a DR or BDR.

**Configuration Prerequisites**

Before configuring the network type of an OSPF interface, perform the following tasks:

- Configuring the network layer address of the interface so that the adjacent node is reachable at network layer
- Performing basic OSPF configuration

**Configuring the Network Type of an OSPF Interface**

<table>
<thead>
<tr>
<th>Table 231</th>
<th>Configure the network type of an OSPF interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the network type of the OSPF interface</td>
<td>ospf network-type { broadcast</td>
</tr>
</tbody>
</table>

By default, the network type of an interface depends on the physical interface.
After an interface has been configured with a new network type, the original network type of the interface is removed automatically.

An adjacency can be established between two interfaces configured as broadcast, NBMA, or P2MP only if the interfaces are on the same network segment.

If the network type of an interface is NBMA or is changed to NBMA, you must use the `peer` command to specify the peer.

If the network type of an interface is P2MP and the `unicast` keyword is specified, an interface sends packets in the unicast mode. In this case, you must use the `peer` command to specify the peer.

### Configuring an NBMA/P2MP Neighbor

When the network type of an interface on the router is one of the following types, you need to specify the IP address of the neighbor router:

- NBMA
- P2MP (required only when the interface sends packets in the unicast mode)

Since the neighbor routers cannot be discovered by broadcasting Hello packets, you must manually specify the IP address of the neighbor router. For an NBMA network, you can determine whether the neighbor has the DR election right.

<table>
<thead>
<tr>
<th>Table 232</th>
<th>Configure NBMA/P2MP neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [router-id router-id ] ]</td>
</tr>
<tr>
<td>Configure an NBMA/P2MP neighbor</td>
<td>peer ip-address [dr-priority dr-priority ]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 233</th>
<th>Configure the DR priority on an OSPF interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the DR priority on the OSPF interface</td>
<td>ospf dr-priority priority</td>
</tr>
</tbody>
</table>

| Remarks | The default DR priority is 1. |

The DR priorities configured by the `ospf dr-priority` command and the `peer` command have different purpose:

- The priority set with the `ospf dr-priority` command is used for actual DR election.
- The priority set with the `peer` command is used to indicate if a neighbor has the right to vote. If you specify the priority to 0 when configuring a neighbor, the local router will believe that the neighbor has no right to vote and sends no packets to the neighbor.
Hello packet to it. This configuration can reduce the number of Hello packets on the network during the election of DR and BDR. However, if the local router is already a DR or BDR, it will send Hello packets to the neighbor whose DR priority is 0 to establish the adjacencies.

**OSPF Route Control**

Perform the following configurations to control the advertisement and reception of the routing information discovered by OSPF and import routing information discovered by other protocols.

**Configuration Prerequisites**

Before configuring OSPF route control, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Completing basic OSPF configuration
- Configuring matching rules for routing information

**Configuring OSPF Route Summarization**

The configuration of OSPF route summarization includes:

- Configuring ABR route summarization,
- Configuring ASBR route summarization for imported routes.

### Table 234 Configure ABR route summarization

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [ router-id router-id ] ]</td>
<td>-</td>
</tr>
<tr>
<td>Enter area view</td>
<td>area area-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable ABR route summarization</td>
<td>abr-summary ip-address mask [ advertise</td>
<td>Required By default, this function is disabled.</td>
</tr>
<tr>
<td></td>
<td>not-advertise ]</td>
<td></td>
</tr>
</tbody>
</table>

### Table 235 Configure ASBR route summarization

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [ router-id router-id ] ]</td>
<td>-</td>
</tr>
<tr>
<td>Enable ASBR route summarization</td>
<td>asbr-summary ip-address mask [ not-advertise</td>
<td>Required This command takes effect only when it is configured on an ASBR. By default, summarization of imported routes is disabled.</td>
</tr>
<tr>
<td></td>
<td>tag value ]</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring OSPF to Filter Received Routes

### Table 236 Configure OSPF to filter received routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [ router-id router-id ] ]</td>
<td>—</td>
</tr>
</tbody>
</table>
OSPF is a dynamic routing protocol based on link state, with routing information hidden in LSAs. Therefore, OSPF cannot filter any advertised or received LSA. In fact, the `filter-policy import` command filters the routes calculated by the SPF algorithm (namely, routes in the OSPF routing table); only the routes passing the filter can be added to the routing table.

### Configuring the OSPF Cost on an Interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter interface view</td>
<td><code>interface interface-type</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Configure the OSPF cost on</td>
<td><code>ospf cost</code> value</td>
<td>Required</td>
</tr>
<tr>
<td>the interface</td>
<td></td>
<td>By default, the interface calculates the OSPF cost according to its current baud rate. For a VLAN interface on the switch, a fixed value of 10 is used.</td>
</tr>
</tbody>
</table>

### Configuring OSPF Route Priority

Since multiple dynamic routing protocols may be running on one router, the problem of route sharing and selection between various routing protocols arises. The system sets a priority for each routing protocol (which you can change manually), and when more than one route to the same destination is discovered by different protocols, the system add the route discovered by the protocol with the highest priority to the routing table.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>`ospf [ process-id</td>
<td>router-id ]`</td>
</tr>
<tr>
<td>Configure OSPF route</td>
<td><code>preference [ asr ] value</code></td>
<td>Optional</td>
</tr>
<tr>
<td>priority</td>
<td></td>
<td>By default, the OSPF route priority is 10 and the priority of OSPF ASE is 150.</td>
</tr>
</tbody>
</table>

### Configuring the Maximum Number of OSPF ECMP Routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>`ospf [ process-id</td>
<td>router-id ]`</td>
</tr>
</tbody>
</table>
Configuring OSPF to Redistribute External Routes

Table 239 Configure the maximum number of OSPF ECMP routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the maximum number of OSPF ECMP routes</td>
<td><code>multi-path-number value</code></td>
<td>Switch 5500:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 3 by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switch 5500G:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 4 by default.</td>
</tr>
</tbody>
</table>

Table 240 Configure OSPF to redistribute external routes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>`ospf [process-id</td>
<td>router-id ]`</td>
</tr>
<tr>
<td>Configure OSPF to redistribute routes from another protocol</td>
<td><code>import-route</code> protocol [ process-id</td>
<td>allow-ibgp ] [ cost value</td>
</tr>
<tr>
<td>Configure OSPF to filter outgoing routes</td>
<td><code>filter-policy</code> acl-number</td>
<td>ip-prefix ip-prefix-name</td>
</tr>
<tr>
<td>Enable OSPF to import the default route</td>
<td><code>default-route-advertise</code> [ always</td>
<td>cost value</td>
</tr>
<tr>
<td>Configure the default parameters for redistributed routes, including cost, interval, limit, tag, and type</td>
<td><code>default</code> cost value</td>
<td>interval seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by default, OSPF does not import the routing information of other protocols.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, OSPF does not filter advertised routes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, OSPF does not import the default route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These parameters respectively default to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Cost: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Interval: 1 (second)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Limit: 1000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Tag: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Type: 2</td>
</tr>
</tbody>
</table>

- The `import-route` command cannot import the default route. To import the default route, you must use the `default-route-advertise` command.
- The filtering of advertised routes by OSPF means that OSPF only converts the external routes meeting the filter criteria into Type-5 or Type-7 LSAs and advertises them.
- When enabling OSPF to import external routes, you can also configure the defaults of some additional parameters, such as cost, limit, tag, and type. A route tag can be used to identify protocol-related information.
You can adjust and optimize an OSPF network in the following aspects:

- By changing the OSPF packet timers, you can adjust the convergence speed of the OSPF network and the network load brought by OSPF packets. On some low-speed links, you need to consider the delay experienced when the interfaces transmit LSAs.

- By adjusting SPF calculation interval, you can mitigate resource consumption caused by frequent network changes.

- In a network with high security requirements, you can enable OSPF authentication to enhance OSPF network security.

- In addition, OSPF supports network management. You can configure the binding of the OSPF MIB with an OSPF process and configure the Trap message transmission and logging functions.

### Configuration Prerequisites

Before adjusting and optimizing an OSPF network, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer

- Configuring basic OSPF functions

### Configuring OSPF Timers

The Hello intervals for OSPF neighbors must be consistent. The value of Hello interval is in inverse proportion to route convergence speed and network load.

The dead time on an interface must be at least four times of the Hello interval on the same interface.

After a router sends an LSA to a neighbor, it waits for an acknowledgement packet from the neighbor. If the router receives no acknowledgement packet from the neighbor within the retransmission interval, it retransmits the LSA to the neighbor.

<table>
<thead>
<tr>
<th>Table 241</th>
<th>Configure OSPF timers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the hello interval on the interface</td>
<td>ospf timer hello seconds</td>
</tr>
<tr>
<td>By default, <strong>p2p</strong> and <strong>broadcast</strong> interfaces send Hello packets every 10 seconds; while <strong>p2mp</strong> and <strong>NBMA</strong> interfaces send Hello packets every 30 seconds.</td>
<td></td>
</tr>
<tr>
<td>Configure the poll interval on the NBMA interface</td>
<td>ospf timer poll seconds</td>
</tr>
<tr>
<td>By default, poll packets are sent every 40 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 30: OSPF CONFIGURATION

Table 241  Configure OSPF timers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the dead time of the neighboring router on the interface</td>
<td>ospf timer dead seconds</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the dead time for the OSPF neighboring router on a p2p or broadcast interface is 40 seconds and that for the OSPF neighboring router on a p2mp or NBMA interface is 120 seconds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the interval for retransmitting an LSA on an interface</td>
<td>ospf timer retransmit interval</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, this interval is five seconds.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Default Hello and Dead timer values will be restored once the network type is changed.

Do not set an LSA retransmission interval that is too short. Otherwise, unnecessary retransmission will occur. LSA retransmission interval must be greater than the round trip time of a packet between two routers.

Table 242  Configure the LSA transmission delay

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure the LSA transmission delay</td>
<td>ospf trans-delay seconds</td>
<td>Required</td>
</tr>
<tr>
<td>By default, the LSA transmission delay is one second.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The transmission of OSPF packets on a link also takes time. Therefore, a transmission delay should be added to the aging time of LSAs before the LSAs are transmitted. For a low-speed link, pay close attention on this configuration.

Configuring the SPF Calculation Interval

Whenever the LSDB of OSPF is changed, the shortest paths need to be recalculated. When the network changes frequently, calculating the shortest paths immediately after LSDB changes will consume enormous resources and affect the operation efficiency of the router. By adjusting the minimum SPF calculation interval, you can lighten the negative affection caused by frequent network changes.

Table 243  Configure the SPF calculation interval

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [ router-id ] ]</td>
<td>—</td>
</tr>
<tr>
<td>Configure the SPF calculation interval</td>
<td>spf-schedule-interval interval</td>
<td>Required</td>
</tr>
<tr>
<td>By default, the SPF calculation interval is five seconds.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Disabling OSPF Packet Transmission on an Interface

To prevent OSPF routing information from being acquired by the routers on a certain network, use the `silent-interface` command to disable OSPF packet transmission on the corresponding interface.

<table>
<thead>
<tr>
<th>Table 244</th>
<th>Disable OSPF packet transmission on an interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td><code>ospf [ process-id [ router-id router-id ] ]</code></td>
</tr>
<tr>
<td>Disable OSPF packet transmission on a specified interface</td>
<td><code>silent-interface</code></td>
</tr>
</tbody>
</table>

- On the same interface, you can disable multiple OSPF processes from transmitting OSPF packets. The `silent-interface` command, however, only applies to the OSPF interface on which the specified process has been enabled, without affecting the interface for any other process.

- After an OSPF interface is set to be in silent status, the interface can still advertise its direct route. However, the Hello packets from the interface will be blocked, and no adjacencies can be established on the interface. This enhances OSPF networking adaptability, thus reducing the consumption of system resources.

Configuring OSPF Authentication

<table>
<thead>
<tr>
<th>Table 245</th>
<th>Configure OSPF authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td><code>ospf [ process-id [ router-id router-id ] ]</code></td>
</tr>
<tr>
<td>Enter OSPF area view</td>
<td><code>area area-id</code></td>
</tr>
<tr>
<td>Configure the authentication mode of the OSPF area</td>
<td>`authentication-mode { simple</td>
</tr>
<tr>
<td>Return to OSPF view</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>Enter interface view</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>Configure the authentication mode of the OSPF interface</td>
<td>`authentication-mode { simple password</td>
</tr>
</tbody>
</table>

- OSPF supports packet authentication and receives only those packets that are successfully authenticated. If packet authentication fails, no adjacencies will be established.

- The authentication modes for all routers in an area must be consistent. The authentication passwords for all routers on a network segment must also be consistent.
### Configuring the MTU Field in DD Packets

By default, an interface uses value 0 instead of its actual MTU value when transmitting DD packets. After the following configuration, the actual interface MTU is filled in the MTU field in DD packets.

**Table 246** Configure to fill the MTU field when an interface transmits DD packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet interface view</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td>Enable the interface to fill in the MTU field when transmitting DD packets</td>
<td>ospf mtu-enable</td>
<td>Required By default, the MTU value is 0 when an interface transmits DD packets. That is, the actual MTU value of the interface is not filled in.</td>
</tr>
</tbody>
</table>

### Enabling OSPF Logging of Neighbor State Changes

**Table 247** Enable OSPF logging of neighbor state changes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter OSPF view</td>
<td>ospf [ process-id [ router-id ] ]</td>
<td>-</td>
</tr>
<tr>
<td>Enable the OSPF logging of neighbor state changes</td>
<td>log-peer-change</td>
<td>Required Disabled by default.</td>
</tr>
</tbody>
</table>

### Configuring OSPF Network Management

**Table 248** Configure OSPF network management (NM)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure OSPF MIB binding</td>
<td>ospf mib-binding process-id</td>
<td>Optional By default, OSPF MIB is bound to the first enabled OSPF process.</td>
</tr>
<tr>
<td>Enable OSPF Trap sending</td>
<td>snmp-agent trap enable ospf [ process-id ] [ ifauthfail</td>
<td>ifcfgerror</td>
</tr>
</tbody>
</table>
### OSPF Configuration Examples

#### Configuring DR/BDR Election

Use OSPF to realize interconnection between devices in a broadcast network. Devices with higher performance should become the DR and BDR to improve network performance. Devices with lower performance are forbidden to take part in DB/BDR election.

#### Network requirements

Table 249  Display and maintain configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the router ID</td>
<td><code>display router id</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display brief information about one or all OSPF processes</td>
<td><code>display ospf [ process-id ] brief</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF statistics</td>
<td><code>display ospf [ process-id ] cumulative</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF LSDB information</td>
<td>`display ospf process-id area-id lsdb [ brief</td>
<td>[ asbr</td>
</tr>
<tr>
<td>Display OSPF peer information</td>
<td>`display ospf [ process-id ] peer [ brief</td>
<td>statistics ]`</td>
</tr>
<tr>
<td>Display OSPF next hop information</td>
<td><code>display ospf [ process-id ] nexthop</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF routing table</td>
<td><code>display ospf [ process-id ] routing</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF virtual links</td>
<td><code>display ospf [ process-id ] vlink</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF request list</td>
<td><code>display ospf [ process-id ] request-queue</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF retransmission list</td>
<td><code>display ospf [ process-id ] retrans-queue</code></td>
<td></td>
</tr>
<tr>
<td>Display the information about OSPF ABR and ASBR</td>
<td><code>display ospf [ process-id ] abr-asbr</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF interface information</td>
<td><code>display ospf [ process-id ] interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF errors</td>
<td><code>display ospf [ process-id ] error</code></td>
<td></td>
</tr>
<tr>
<td>Display OSPF ASBR summarization information</td>
<td><code>display ospf [ process-id ] asbr-summary [ ip-address mask ]</code></td>
<td></td>
</tr>
<tr>
<td>Reset OSPF process(es)</td>
<td>`reset ospf { all</td>
<td>process-id }`</td>
</tr>
<tr>
<td>Clear the statistics of one or all OSPF processes</td>
<td>`reset ospf statistics { all</td>
<td>process-id }`</td>
</tr>
</tbody>
</table>

---

Use OSPF to realize interconnection between devices in a broadcast network. Devices with higher performance should become the DR and BDR to improve network performance. Devices with lower performance are forbidden to take part in DB/BDR election.
Based on the customer requirements and networking environment, assign proper priorities to interfaces.

**Network diagram**

*Figure 90*  Network diagram for DR/BDR election

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Router ID</th>
<th>Interface priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int1</td>
<td>196.1.1.1/24</td>
<td>1.1.1.1</td>
<td>100</td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int1</td>
<td>196.1.1.2/24</td>
<td>2.2.2.2</td>
<td>0</td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int1</td>
<td>196.1.1.3/24</td>
<td>3.3.3.3</td>
<td>2</td>
</tr>
<tr>
<td>Switch D</td>
<td>Vlan-int1</td>
<td>196.1.1.4/24</td>
<td>4.4.4.4</td>
<td>1</td>
</tr>
</tbody>
</table>

**Configuration procedure**

# Configure Switch A.

```plaintext
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

# Configure Switch B.

```plaintext
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

# Configure Switch C.

```plaintext
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 196.1.1.3 255.255.255.0
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface1] quit
```
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255

# Configure Switch D.

<SwitchD> system-view
[SwitchD] interface Vlan-interface 1
[SwitchD-Vlan-interface1] ip address 196.1.1.4 255.255.255.0
[SwitchD-Vlan-interface1] quit
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255

On Switch A, run the **display ospf peer** command to display its OSPF peers. Note that Switch A has three peers.

The state of each peer is full, which means that adjacency is established between Switch A and each peer. Switch A and Switch C must establish adjacencies with all the switches on the network so that they can serve as the DR and BDR respectively on the network. Switch A is DR, while Switch C is BDR on the network. All the other neighbors are DR others (This means that they are neither DRs nor BDRs).

# Change the priority of Switch B to 200.

<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200

On Switch A, use the **display ospf peer** command to display its OSPF neighbors. Note that the priority of Switch B has been changed to 200, but it is still not a DR.

The current DR is changed only when it is offline. Shut down Switch A, and use the **display ospf peer** command on Switch D to display its neighbors. Note that the original BDR (Switch C) becomes the DR and Switch B becomes BDR now.

If all Ethernet Switches on the network are removed from and then added to the network again, Switch B will be elected as the DR (with a priority of 200), and Switch A will be the BDR (with a priority of 100). Shutting down and restarting all the switches will bring about a new round of DR/BDR election on the network.

### Configuring OSPF

#### Virtual Link

**Network requirements**

Devices in the network run OSPF to realize interconnection. The network is split into three areas: one backbone area and two non-backbone areas (Area 1 and Area 2). Area 2 has no direct connection to the backbone, and it has to reach the backbone through Area 1. The customer hopes that Area 2 can interconnect with other two areas.

Based on the customer requirements and networking environment, use a virtual link to connect Area 2 to the backbone area.
Network diagram

Figure 91  Network diagram for OSPF virtual link configuration

![Network diagram for OSPF virtual link configuration]

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP interface</th>
<th>Router ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int1</td>
<td>196.1.1.1/24</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int1</td>
<td>196.1.1.2/24</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td></td>
<td>Vlan-int2</td>
<td>197.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int1</td>
<td>152.1.1.1/24</td>
<td>3.3.3.3</td>
</tr>
<tr>
<td></td>
<td>Vlan-int2</td>
<td>197.1.1.1/24</td>
<td></td>
</tr>
</tbody>
</table>

Configuration procedure

# Configure Switch A.

```bash
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255

# Configure Switch B.

<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 197.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```
Troubleshooting OSPF Configuration

Unable to Establish a Neighbor Relationship between Routers

Symptom
No neighbor relationship can be established between neighboring routers.

Analysis
1. Verify that the routers work normally at the link layer.
2. Verify that the conditions for establishing a neighbor relationship are satisfied.
   - OSPF parameters on the interconnected interfaces must be consistent.
   - Area IDs on the interconnected interfaces must be the same.
   - Network ID and subnet masks of the interconnected interfaces must be consistent. (P2P networks and virtual link are excluded.)
   - The interconnected interfaces have the same type of network.
   - If the network type of the interface on the local router is NBMA, a neighbor must be specified by using the `peer` command.

Solution
Perform the following procedure.

1. Use the `display ip interface brief` command to verify that the link layer works normally.
2. Use the `ping` command to check network layer connectivity.
3. Use the `display ospf interface` command to view the OSPF interface configuration.
4 If the network type of an interface is NBMA, use the `display current-configuration configuration ospf` command to verify that a neighbor is specified for the router.

5 Use the `display ospf brief` command to check that the OSPF timers are consistent with those on the neighbor and that the dead time of the neighbor is four times the Hello interval.

6 Use the `display ospf peer` command to view neighbors.

### Unable to Learn a Complete Network Topology

**Symptom**
The router running OSPF is unable to learn a complete network topology.

**Analysis**
Perform the following procedure to make analyses:

1 If multiple areas are configured on the router, check that one is specified as the backbone area.

2 Check that the backbone area is fully meshed.

3 Check that the backbone area is not configured as a Stub area or NSSA area.

4 Check that no virtual links are configured for the backbone area.

5 For a Stub area, check that the Stub attributes are configured for all routers in the area.

6 For an NSSA area, check that the NSSA attributes are configured for all routers in the area.

7 Check that Stub or NSSA areas are not a transit area of any virtual link. Virtual links cannot pass through a Stub or NSSA area.

**Solution**
Perform the following procedure:

1 Use the `display ospf peer` command to view the OSPF neighbor status.

2 Use the `display ospf interface` command to view the OSPF configuration on an interface.

3 Use the `display ospf lsdb` command to view the LSDB information.

4 Use the `display current-configuration configuration ospf` command to view area configurations.

5 If a virtual link is configured, use the `display ospf vlink` command to check that the OSPF virtual link is normal.
BGP Overview

Border gateway protocol (BGP) is a dynamic routing protocol designed to be employed among autonomous systems (AS). An AS is a group of routers that adopt the same routing policy and belong to the same technical management department.

Four versions of BGP exist: BGP-1 (described in RFC1105), BGP-2 (described in RFC1163), BGP-3 (described in RFC1267), and BGP-4 (described in RFC1771). As the actual internet exterior routing protocol standard, BGP-4 is widely employed between internet service providers (ISP).

BGP is featured by the following.

- Unlike interior gateway protocols (IGP) such as OSPF (open shortest path first), RIP (routing information field), and so on, BGP is an exterior gateway protocol (EGP). It does not focus on discovering and computing routes but controlling the route propagation and choosing the optimal route.
- BGP uses TCP as the transport layer protocol (with the port number being 179) to ensure reliability.
- BGP supports classless inter-domain routing (CIDR).
- With BGP employed, only the changed routes are propagated. This saves network bandwidth remarkably and makes it feasible to propagate large amount of route information across the Internet.
- The AS path information used in BGP eliminates route loops thoroughly.
- In BGP, multiple routing policies are available for filtering and choosing routes in a flexible way.
- BGP is extendible to allow for new types of networks.

In BGP, the routers that send BGP messages are known as BGP speakers. A BGP speaker receives and generates new routing information and advertises the information to other BGP speakers. When a BGP speaker receives a route from other AS, if the route is better than the existing routes or the route is new to the
BGP speaker, the BGP speaker advertises the route to all other BGP speakers in the AS it belongs to.

A BGP speaker is known as the peer of another BGP speaker if it exchanges messages with the latter. A group of correlated peers can form a peer group.

BGP can operate on a router in one of the following forms.

- IBGP (Internal BGP)
- EBGP (External BGP)

When BGP runs inside an AS, it is called interior BGP (IBGP); when BGP runs among different ASs, it is called exterior BGP (EBGP).

**BGP Message Type**

**Format of a BGP packet header**

BGP is message-driven. There are five types of BGP packets: Open, Update, Notification, Keepalive, and Route-refresh. They share the same packet header, the format of which is shown by Figure 92.

**Figure 92** Packet header format of BGP messages

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>15</th>
<th>23</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Marker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Length</td>
<td></td>
<td>Type</td>
</tr>
</tbody>
</table>

The fields in a BGP packet header are described as follows.

- **Marker**: 16 bytes in length. This field is used for BGP authentication. When no authentication is performed, all the bits of this field are 1.
- **Length**: 2 bytes in length. This field indicates the size (in bytes) of a BGP packet, with the packet header counted in.
- **Type**: 1 byte in length. This field indicates the type of a BGP packet. Its value ranges from 1 to 5, which represent Open, Update, Notification, Keepalive, and Route-refresh packets. Among these types of BGP packets, the first four are defined in RFC1771, and the rest one is defined in RFC2918.

**Open**

Open massage is used to establish connections between BGP speakers. It is sent when a TCP connection is just established. Figure 93 shows the format of an Open message.
The fields are described as follows.

- **Version**: BGP version. As for BGP-4, the value is 4.
- **My Autonomous System**: Local AS number. By comparing this filed of both sides, a router can determine whether the connection between itself and the BGP peer is of EBGP or IBGP.
- **Hold time**: Hold time is to be determined when two BGP speakers negotiate for the connection between them. The Hold times of two BGP peers are the same. A BGP speaker considers the connection between itself and its BGP peer to be terminated if it receives no Keepalive or Update message from its BGP peer during the hold time.
- **BGP Identifier**: The IP address of a BGP router.
- **Opt Parm Len**: The length of the optional parameters. A value of 0 indicates no optional parameter is used.
- **Optional Parameters**: Optional parameters used for BGP authentication or multi-protocol extensions.

### Update

Update message is used to exchange routing information among BGP peers. It can propagate a reachable route or withdraw multiple pieces of unreachable routes. Figure 94 shows the format of an Update message.

An Update message can advertise a group of reachable routes with the same path attribute. These routes are set in the NLRI (network layer reachability information) field. The Path Attributes field carries the attributes of these routes, according to which BGP chooses routes. An Update message can also carry multiple unreachable routes. The withdrawn routes are set in the Withdrawn Routes field.

The fields of an Update message are described as follows.
■ Unfeasible Routes Length: Length (in bytes) of the unreachable routes field. A value of 0 indicates that there is no Withdrawn Routes filed in the message.
■ Withdrawn Routes: Unreachable route list.
■ Total Path Attribute Length: Length (in bytes) of the Path Attributes field. A value of 0 indicates that there is no Path Attributes filed in the message.
■ Path Attributes: Attributes list of all the paths related to NLRI. Each path attribute is a TLV (Type-Length-Value) triplet. In BGP, loop avoidance, routing, and protocol extensions are implemented through these attribute values.
■ NLRI (Network Layer Reachability Information): Contains the information such reachable route suffix and the corresponding suffix length.

**Notification**

When BGP detects error state, it sends the Notification message to peers and then tear down the BGP connection. Figure 95 shows the format of an Notification message.

![Figure 95](BGP_Notification_message_format.png)

The fields of a Notification message are described as follows.

■ Error Code: Error code used to identify the error type.
■ Error Subcode: Error subcode used to identify the detailed information about the error type.
■ Data: Used to further determine the cause of errors. Its content is the error data which depends on the specific error code and error subcode. Its length is unfixed.

**Keepalive**

In BGP, Keepalive message keeps BGP connection alive and is exchanged periodically. A BGP Keepalive message only contains the packet header. No additional fields is carried.

**Route-refresh**

Route-refresh messages are used to notify the peers that the route refresh function is available and request the peers to resend the routing information of the specified address family. Figure 96 shows the format of a route-refresh message.

![Figure 96](Route-refresh_message_format.png)

The fields of a route-refresh message are described as follows.
BGP Overview

- AFI: Address family identifier
- Res: Reserved. This field must not be set.
- SAFI: Subsequent address family identifier

**BGP Route Attributes**

**Routes attributes classification**

BGP route attributes describe route, so that BGP can filter and choose the routes. In fact, all the BGP route attributes can be classified into the following four categories.

- Well-known mandatory attributes, which can be identified by any BGP routers. Route attributes of this type are carried in Update messages. Without these attributes, routing information goes wrong.
- Well-known discretionary attributes, which can be identified by any BGP routers. An Update message can travel with or without this type of attributes.
- Optional transitive attributes, which can be transmitted among ASs. Although attributes of this type may not be supported by any BGP routers, routes with them can still be received and be forwarded to BGP speakers.
- Optional non-transitive attributes, which is dropped on the BGP routers that do not support them. In this case, the attributes are not forwarded to other BGP routers.

Table 5-1 lists basic BGP route attributes and the categories they belong to.

**Table 5-1 BGP route attributes and the corresponding categories**

<table>
<thead>
<tr>
<th>BGP route attribute</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIGIN</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>AS_PATH</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>NEXT_HOP</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>LOCAL_PREF</td>
<td>Well-known discretionary</td>
</tr>
<tr>
<td>ATOMIC_AGGREGATE</td>
<td>Well-known discretionary</td>
</tr>
<tr>
<td>AGGREGATOR</td>
<td>Optional transitive</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>Optional transitive</td>
</tr>
<tr>
<td>MULTI_EXIT_DISC(MED)</td>
<td>Optional non-transitive</td>
</tr>
<tr>
<td>ORIGINATOR_ID</td>
<td>Optional non-transitive</td>
</tr>
<tr>
<td>CLUSTER_LIST</td>
<td>Optional non-transitive</td>
</tr>
</tbody>
</table>

**Primary route attributes**

- **ORIGIN:**
  - The ORIGIN attribute holds the source of routing information. It indicates how a route becomes a BGP route. The following describes the possible values of the ORIGIN attribute.
- **IGP**: BGP routes with their ORIGIN attributes being IGP have the highest priority. They are added to the BGP routing table through the `network` command.

- **EGP**: BGP routes with their ORIGIN attributes being EGP are obtained through EGP.

- **Incomplete**: BGP routes with their ORIGIN attributes being Incomplete have the least priority. This value does not indicate that the BGP route is unreachable; it means the source of the BGP route cannot be determined. The ORIGIN attribute of a BGP route imported through the `import-route` command is Incomplete.

- **AS_PATH**: The AS_PATH attribute holds the numbers of all the ASs that a route passes from the source to the destination. AS numbers in this attribute are in the order the route passes the ASs. Before a BGP speaker advertises a route to the BGP speakers of other ASs, it adds the local AS number to the head of the AS number queue in the AS_PATH attribute. According to the AS_PATH attribute of a received BGP route, a router can retrieve the information about the ASs the route passes. In AS_PATH attribute, AS numbers are listed by the distances between the ASs and the local AS. The number of the AS that is closest to the local AS is listed in the head, as shown in Figure 97.

![Figure 97: AS_PATH attribute](image)

Normally, a router with BGP employed discards the routes that contain local AS number in the AS_PATH attribute. This eliminates routing loops.

You can use the `peer allow-as-loop` command to allow AS number repetition to meet some special needs.

AS_PATH attribute can also be used to choose and filter routes. BGP chooses the routes containing less AS numbers with shorter path under the same
circumstances. For example, in Figure 97, the BGP router in AS50 will choose the path passing through AS40 as the route to the router in AS 10.

In some applications, you can increase the number of AS numbers a BGP route contains through routing policy to control BGP routing in a flexible way. By configuring AS path filtering list, you can have BGP routes filtered by the AS numbers contained in the AS-Path attribute.

- **NEXT_HOP**: Different from that of the IGP, the NEXT_HOP attribute of a BGP route does not necessarily hold the IP address of the neighbor router. The NEXT_HOP attribute is set in the following ways.
  - When a BGP speaker advertises a route generated by itself to all its neighbors, it sets the NEXT_HOP attribute of the routing information to the address of its own interface connecting to the peer.
  - When a BGP speaker sends a received route to one of its EBGP peer, it sets the NEXT_HOP attribute of the routing information to the address of its interface connecting to the EBGP peer.
  - When a BGP speaker sends a route received from one of its EBGP peer to one of its IBGP neighbor, it does not change the NEXT_HOP attribute of the routing information. But with load balancing enabled, the NEXT_HOP attribute is changed when the BGP route is sent to a IBGP neighbor.

**Figure 98** The NEXT_HOP attribute

- **MED (MULTI_EXIT_DISC)**: The MED attribute is only valid between two neighboring ASs. The AS receiving this attribute will not advertise this attribute to a third AS.

The MED attribute is used to determine the optimal route for traffic flows to enter an AS. It acts the same as the metrics used in IGP. For multiple routes a BGP router receives from different EBGP peers, if they have the same destination address but different next hops, the route with the smallest MED value is chosen as the optimal route provided other conditions are the same. As shown in Figure 99, Router B is chose as the ingress for traffic from AS 10 to AS 20.
CHAPTER 31: BGP CONFIGURATION

Figure 99  MED attribute

Normally, BGP only compares the MED attribute values of the routes received from the same AS.

You can force BGP to compare MED values of routes coming from different ASs.

- **LOCAL_PREF**: The LOCAL_PREF attribute is only valid among IBGP peers. It is not advertised to other ASs. It indicates the priority of a BGP router.

  LOCAL_PREF attribute is used to determine the optimal route for traffic leaving an AS. For multiple routes a BGP receives from different IBGP peers, if they have the same destination address but different next hops, the route with the smallest LOCAL_PREF value is chosen as the optimal route provided other conditions are the same. As shown in Figure 100, RouterC is chose as the egress for traffic from AS 20 to AS 10.

Figure 100  LOCAL_PREF attribute

- **COMMUNITY**: The Community attribute is used to simplify routing policy application and ease the maintenance and management of routing policy. Community is a set of destination addresses with the same features. It is not
restricted to physical boundary and is independent of AS. The Community attribute can be one of the following.

- **INTERNET.** By default, the value of the COMMUNITY attributes of all routes is INTERNET. That is, all routes belong to the Internet community by default. Routes with this attribute can be advertised to all BGP peers.

- **No_EXPORT.** Routes with this attribute cannot be sent to routers outside the local AS. With the presence of the confederation, routes of this kind cannot be advertised outside the confederation, they can only be advertised in the sub-ASs in the confederation. (For information about confederation, “Configuring a Large-Scale BGP Network” on page 354.

- **No_ADVERTISE.** Routes with this attribute cannot be advertised to any other BGP peers after being received by a BGP router.

- **No_EXPORT_SUBCONFED.** Routes with this attribute can neither be advertised outside the local AS nor be advertised to other sub-ASs inside the confederation after being received.

### BGP Routing Policy

**BGP routing policy**

- A BGP router filters routes in the following order.

  - Drops the NEXT_HOP unreachable route.

  - With Prefered-value specified, chooses the route with highest Prefered-value value.

  - Prefers the route with highest LOCAL_PREF value.

  - Prefers the routes starting from the local router.

  - Prefers the route with the shortest AS path.

  - Chooses routes in the order of the route ORIGIN type, that is, the order of IGP, EGP, and Incomplete.

  - Prefers the route with the lowest MED value.

  - Chooses the route learnt from EBGP, the route learnt from confederation and the route learnt from the IBGP in turn.

  - Prefers the route with the smallest ORIGINATOR ID.

  - Prefers the route with the smallest router ID.

### BGP route advertising policy

A BGP router adopts the following policies to advertise routes.

- Sends the optimal route to its peers when multiple valid routes exist.

- Sends only the routes used by itself to its peers.

- Sends all the EBGP routes to all its BGP peers, including the EBGP peers and IBGP peers.

- Does not send IBGP routes to its IBGP peers.

- Sends IBGP routes to its EBGP peers.

- Sends all its BGP routes to the new peer once a new BGP connection is established.
Problems in Large-Scale BGP Networks

Route summarization

BGP routing tables in a large-scale network may be huge in size. Route summarization can largely diminish the size of a routing table.

Route summarization aggregates multiple routes to one route. It enables a BGP router to replace multiple specific routes with one summary route.

The switches support automatic route summarization and manual route summarization. In the manual route summarization mode, you can control the attribute of the summary routes and determine whether to send the specific routes or not.

BGP route dampening

BGP route dampening is used to solve the problem of route instability. Route instability mainly takes the form of route flaps, that is, a route appears and disappears repeatedly in the routing table.

When route flaps occur, a route sends route update to its neighbors. Routers receiving the update packets calculate the route over again and renew the routing table. Therefore, frequent route flaps consume much bandwidth and CPU time. They even affect the operation of network.

In most cases, BGP is applied in complicated networks where route changes are frequent. In order to avoid the unfavorable affection caused by route flaps, BGP uses route dampening to suppress the instable routes.

BGP route dampening uses penalty value to judge the stability of a route. A higher penalty value indicates a more instable route. Each time a route flaps, BGP adds a certain penalty value (fixed to 1000) to the route. When the penalty value excesses the suppression threshold, the route will be suppressed and will neither be added to the routing table nor send update packets to other BGP peers.

The penalty value of a suppressed route is decreased by half in each specific period known as half-life. When the penalty value is decreased to a value less than the reuse threshold, the route gets valid and is added to the routing table again. At the same time, the BGP router sends corresponding update packets to its BGP peers.
Peer group

Peer group is a set of peers that are the same in certain attributes. When a peer joins into a peer group, the peer obtains the same configurations with those of the peer group. When the configuration of a peer group changes, those of the group members change accordingly.

A large-scale network can contain large amount of peers, lot of which adopt the same policies. Peer group simplifies your configuration when you configure peers adopting the same policy.

As the peers in a peer group adopt the same route updating policy, peer group gains more efficiency in route advertising.

**Caution:** If a BGP peer and the peer group containing the BGP peer are configured differently, the last configuration takes effect.

Community

Different form peer group, you can apply the same policy to BGP routers residing in different ASs through community. Community is a route attribute transmitted among BGP peers. It is independent of AS.

Before sending a route with the COMMUNITY attribute to its peers, a BGP router can change the original COMMUNITY attribute of the route.

Besides the well-known COMMUNITY attributes, you can also use the COMMUNITY attributes list to customize extended COMMUNITY attributes, so as to control the routing policy with more flexibility.
Router reflector

To ensure the connectivity among the IBGP peers in an AS, you need to make the IBGP peers fully connected. For an AS with the number of the routers in it being n, you need to establish at least n*(n-1)/2 IBGP connections to make them fully connected. This requires large amount of network resources and CPU time if large amount of IBGP peers exist in the AS.

You can decrease the use of network resources and CPU time through route reflection in this case. That is, use a router as a router reflector (RR) and establish IBGP connections between the RR and other routers known as clients. Routing information exchanged between the clients is passed/reflected by the RR. This eliminates the need to establish IBGP connections among the clients.

Note that a BGP router which is neither the RR nor a client is called a non-client. Non-clients and the RR must be fully connected, as shown in Figure 102.

**Figure 102**  Diagram for the route reflector

An RR and all its clients form a cluster. To ensure network reliability and avoid single-point failure, you can configure more than one RR in a cluster. In this case, make sure all the RRs in the cluster are configured with the same cluster ID to avoid routing loops. Figure 103 shows a cluster containing two RRs.
RR is unnecessary for clients that are already fully connected. You can disable routing information reflection using corresponding commands provided by the switches.

The configuration to disable routing information reflection only applies to clients. That is, routing information can still be reflected between a client and a non-client even if you disable routing information reflection.

Confederation

Confederation is another way to limit the number of IBGP connections in an AS. It divides an AS into multiple sub-ASs. The IBGP peers in each sub-AS are fully connected. The sub-ASs are connected through EBGP connections, Figure 104 shows a confederation implementation.
To a BGP speaker that does not belong to any confederation, the sub-ASs of a confederation are a whole, and the information about the sub-ASs is invisible to the BGP speaker. The confederation ID, which is usually the corresponding AS number, uniquely identifies a confederation. In Figure 104, AS 200 is a confederation ID.

The disadvantage of confederation is that when an AS changes from non-confederation to confederation, configurations are needed on the routers, and the topology changes.

In a large-scale BGP network, router reflector and confederation can be used simultaneously.

**MP-BGP**

**MP-BGP overview**

BGP-4 can only process IPv4 routing information. It is not applicable to the applications using other network layer protocols (such as IPv6) when inter-AS routing information exchange is required.

To support multiple network layer protocols, IETF extends BGP-4 to MP-BGP. MP-BGP standard is described in RFC2858, multiprotocol extensions for BGP-4.a MP-BGP is backward compatible. It enables communications to routers with BGP-4 employed.

**Extended attribute of MP-BGP**

Of different types of BGP-4 packets, all the information concerning to IPv4 are carried by Update packets. The information is hold by NLRI, NEXT_HOP (in the AS_PATH attribute), and AGGREGATOR (in the AS_PATH attribute). (The AGGREGATOR attribute contains the IP address of the BGP speaker that generates a summarized route.)
To support multiple network layer protocols, NLRI and NEXT_HOP need to hold the information about the network layers. To achieve this, the following two path-related attributes are added in MP-BGP.

- **MP_REACH_NLRI**, which stands for multiprotocol reachable NLRI and is used to advertise reachable routes and next hop information.
- **MP_UNREACH_NLRI**, which stands for multiprotocol unreachable NLRI and is used to withdraw unreachable routes.

The two attributes are all of the optional non-transitive type. Therefore, BGP speakers that do not support multiple protocols ignore the information carried in the two attributes and do not pass the information to their neighbors.

**Protocol Standard**

Protocol standards concerning BGP are:

- RFC1771: A border gateway protocol 4 (BGP-4)
- RFC2858: Multiprotocol extensions for BGP-4
- RFC3392: Capabilities advertisement with BGP-4
- RFC2918: Route refresh capability for BGP-4
- RFC2439: BGP route flap damping
- RFC1997: BGP communities attribute
- RFC2796: BGP route reflection
- RFC3065: Autonomous system confederations for BGP

Others are still in draft, such as the graceful restart feature and the extended COMMUNITY attribute.

**Basic BGP Configuration**

This section describes basic BGP configuration.

As BGP is based on TCP connections, you need to assign IP addresses for BGP peers. BGP peers are not necessarily the neighbor routers. A BGP peer can also be obtained through logical links. Loopback interfaces are usually used to establish BGP connections for stability.

**Configuration Prerequisites**

Before performing basic BGP configuration, you need to ensure network layer connectivity between adjacent nodes.

Before performing basic BGP configuration, make sure the following are available.

- Local AS number
- IPv4 address and AS number of the peers
- Source interface of update packets (optional).
Configuring BGP Multicast Address Family

Follow the steps in Table 251 to configure BGP multicast address family.

Table 251 Configuring BGP Multicast Address Family

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Enter multicast address family view</td>
<td>ipv4-family multicast</td>
<td>Required</td>
</tr>
</tbody>
</table>

Configuration in multicast address family view is similar to that in BGP view. So, unless otherwise noted, refer to “Basic BGP Configuration” on page 343 for information about the configuration in multicast address family view. For information about the related commands, refer to the command manual of this manual. The following configurations are all for BGP view.

Configuring Basic BGP Functions

Follow the steps in Table 252 to configure basic BGP functions.

Table 252 Configuring Basic BGP Functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td></td>
<td>—</td>
</tr>
<tr>
<td>Enable BGP and enter BGP view</td>
<td>bgp as-number</td>
<td>Required</td>
</tr>
<tr>
<td>Specify the AS number for the BGP peers</td>
<td>peer group-name as-number</td>
<td>By default, a peer is not assigned an AS number.</td>
</tr>
<tr>
<td>Assign a description string for a BGP peer/a BGP peer group</td>
<td>peer {group-name</td>
<td>ip-address} description description-text</td>
</tr>
<tr>
<td>Activate a specified BGP peer</td>
<td>peer {group-name</td>
<td>ip-address} enable</td>
</tr>
<tr>
<td>Enable BGP logging</td>
<td>log-peer-change</td>
<td>Optional</td>
</tr>
<tr>
<td>Specify the source interface for route update packets</td>
<td>peer {group-name</td>
<td>ip-address} connect-interface interface-type interface-number</td>
</tr>
<tr>
<td>Allow routers that belong to non-directly connected networks to establish EBGP connections.</td>
<td>peer group-name ebgp-max-hop [hop-count ]</td>
<td>Optional</td>
</tr>
</tbody>
</table>

You can configure the maximum hops of EBGP connection by specifying the hop-count argument.

To configure basic functions of BGP peer group, you need to create the BGP peer group first. Refer to “Configuring BGP Peer Group” on page 354 for information about creating a BGP peer group.
In order for route updating packets being sent even if problems occur on interfaces, you can configure the source interfaces of route update packets as a loopback interface.

Normally, EBGP peers are connected through directly connected physical links. If no such link exists, you need to use the peer ebgp-max-hop command to allow the peers to establish multiple-hop TCP connections between them. If loopback interfaces are used to establish connections between EBGP peers, the peer ebgp-max-hop command is unnecessary.

Note the following:

- It is required to specify for a BGP router a router ID, a 32-bit unsigned integer and the unique identifier of the router in the AS.
- You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is: If loopback interface addresses are available, the last configured loopback interface IP address is used as the router ID; otherwise, the first configured interface IP address is used as the router ID. 3Com recommends that you specify a loopback interface address as the router ID to enhance network reliability.
- Router IDs can be re-selected. A re-selected router ID takes effect only after the BGP process is restarted.

### Configuring How to Advertise and Receive Routing Information

#### Configuration Prerequisites

- Enable the basic BGP functions before configuring the way to advertise/receive BGP routing information.
- Make sure the following information is available when you configure the way to advertise/receive BGP routing information.
  - The summarization mode, and the summary route.
  - Access list number
  - Filtering direction (advertising/receiving) and the route policies to be adopted.
  - Route dampening settings, such as half-life and the thresholds.

#### Importing Routes

With BGP employed, an AS can send its interior routing information to its neighbor ASs. However, the interior routing information is not generated by BGP, it is obtained by importing IGP routing information to BGP routing table. Once IGP routing information is imported to BGP routing table, it is advertised to BGP peers. You can filter IGP routing information by routing protocols before the IGP routing information is imported to BGP routing table.

Follow the steps in Table 253 to import routes:

<table>
<thead>
<tr>
<th>Table 253 Importing Routes</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>system-view</td>
<td></td>
</tr>
</tbody>
</table>
Caution:

- If a route is imported to the BGP routing table through the import-route command, its ORIGIN attribute is incomplete.
- The routes of the specified network segment to be advertised with the network command must be in the local IP routing table. You can use routing policy to control route advertising with more flexibility.
- The ORIGIN attribute of the routes injected to the BGP routing table with the network command is IGP.

Configuring BGP Route Summarization

In a medium/large-sized BGP network, you can reduce the number of the routes to be advertised to BGP peers through route summarization.

Route summarization means that subnet routes in a natural network are summarized with a natural network which is sent to other networks. This function can reduce the number of routing updates advertised to peers and the sizes of peer routing tables.

BGP supports two route summarization modes: automatic summarization mode and manual summarization mode.

- Automatic summarization mode, where IGP sub-network routes imported by BGP are summarized. In this mode, BGP advertises a natural network segment instead of subnet-specific routing information. For example, if automatic route summarization is configured, the routes 160.10.1.0/24, 160.10.2.0/24, and 160.10.3.0/24 in the routing table are summarized with 160.10.0.0/16 which is advertised instead.
- Manual summarization mode, where local BGP routes are summarized. In this mode, BGP summarizes multiple routes with one route.

Note the following:

- Default routes cannot be summarized in the automatic mode.
- The routes injected with the network command cannot be summarized in the automatic mode.
- Manual summary routes enjoy higher priority than automatic ones.
Follow the steps in Table 254 to configure BGP route summarization:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure BGP route summarization:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Enable automatic route summarization</td>
<td>summary</td>
<td>Required By default, routes are not summarized.</td>
</tr>
<tr>
<td>2 Configure a summary route</td>
<td>aggregate ip-address mask [ as-set</td>
<td>attribute-policy route-policy-name</td>
</tr>
</tbody>
</table>

Follow the steps in Table 255 to enable default route advertising:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Enable default route advertising</td>
<td>peer group-name default-route-advertise [ route-policy route-policy-name ]</td>
<td>Required By default, a BGP router does not send default routes to a specified peer/peer group.</td>
</tr>
</tbody>
</table>

With the peer default-route-advertise command executed, no matter whether the default route is in the local routing table or not, a BGP router sends a default route, whose next hop address is the local address, to the specified peer or peer group.

Follow the steps in Table 256 to configure BGP route distribution filtering policies:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Filter the advertised routes</td>
<td>filter-policy { acl-number</td>
<td>ip-prefix ip-prefix-name } export [ protocol [ process-id ] ]</td>
</tr>
<tr>
<td>Specify a route advertising policy for the routes advertised to a peer group</td>
<td>peer group-name route-policy route-policy-name export</td>
<td>Required By default, no route advertising policy is specified for the routes advertised to a peer group.</td>
</tr>
</tbody>
</table>
CHAPTER 31: BGP CONFIGURATION

Caution:

- Only the routes that pass the specified filter are advertised.
- A peer group member uses the same outbound route filtering policy as that of the peer group it belongs to. That is, a peer group adopts the same outbound route filtering policy.

Configuring BGP Route Reception Filtering Policies

Follow the steps in Table 257 to configure BGP route reception filtering policies:

Table 256 Configuring BGP Route Distribution Filtering Policies

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the routing information to be advertised to a peer group:</td>
<td></td>
<td>By default, a peer group has no peer group-based ACL BGP route filtering policy, AS path ACL-based BGP route filtering policy, or IP prefix list-based BGP route filtering policy configured.</td>
</tr>
<tr>
<td>1 Specify an ACL-based BGP route filtering policy for a peer group</td>
<td>peer group-name filter-policy acl-number export</td>
<td></td>
</tr>
<tr>
<td>2 Specify an AS path ACL-based filtering policy for a peer group</td>
<td>peer group-name as-path-acl acl-number export</td>
<td></td>
</tr>
<tr>
<td>3 IP prefix-based BGP route filtering policy for a peer group</td>
<td>peer group-name ip-prefix ip-prefix-name export</td>
<td></td>
</tr>
</tbody>
</table>

Table 257 Configuring BGP Route Reception Filtering Policies

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Filter the received global routing information</td>
<td>filter-policy { acl-number</td>
<td>gateway ip-prefix-name</td>
</tr>
<tr>
<td>Specify a route filtering policy for routes coming from a peer/peer group</td>
<td>peer { group-name</td>
<td>ip-address } route-policy policy-name import</td>
</tr>
<tr>
<td>Filter the routing information received from a peer/peer group:</td>
<td></td>
<td>Required By default, no ACL-based BGP route filtering policy, AS path ACL-based BGP route filtering policy, or IP prefix list-based BGP route filtering policy is configured for a peer/peer group.</td>
</tr>
<tr>
<td>1 Specify an ACL-based BGP route filtering policy for a peer/peer group</td>
<td>peer { group-name</td>
<td>ip-address } filter-policy acl-number import</td>
</tr>
<tr>
<td>2 Specify an AS path ACL-based route filtering policy for a peer/peer group</td>
<td>peer { group-name</td>
<td>ip-address } as-path-acl acl-number import</td>
</tr>
<tr>
<td>3 Specify an IP prefix list-based BGP route filtering policy for a peer/peer group</td>
<td>peer { group-name</td>
<td>ip-address } ip-prefix ip-prefix-name import</td>
</tr>
</tbody>
</table>
Caution:
- Routes received by a BGP router are filtered, and only those matching the specified ACLs are added to the routing table.
- A peer group member and the peer group can use different inbound routing policies, that is, peers of a peer group can use different route filtering policies for receiving routing information.

Disable BGP-IGP Route Synchronization

Follow the steps in Table 258 to disable BGP-IGP route synchronization:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Disable BGP-IGP route synchronization</td>
<td>undo synchronization</td>
<td>Required By default, BGP routes and IGP routes are not synchronized.</td>
</tr>
</tbody>
</table>

Caution: BGP-IGP route synchronization is not supported on the switches.

Configuring BGP Route Dampening

Route dampening is used to solve the problem of route instability. Route instability mainly refers to route flapping. A route flaps if it appears and disappears repeatedly in the routing table. Route flapping increases the number of BGP update packets, consumes the bandwidth and CPU time, and even decreases network performance.

Assessing the stability of a route is based on the behavior of the route in the previous time. Once a route flaps, it receives a certain penalty value. When the penalty value reaches the suppression threshold, this route is suppressed. The penalty value decreases with time. When the penalty value of a suppressed route decreases to the reuse threshold, the route gets valid and is thus advertised again.

BGP dampening suppresses unstable routing information. Suppressed routes are neither added to the routing table nor advertised to other BGP peers.

Follow the steps in Table 259 to configure BGP route dampening:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>-</td>
</tr>
</tbody>
</table>
### CHAPTER 31: BGP CONFIGURATION

#### Configuring BGP

**Route Attributes**

**Configuration Prerequisites**

Before configuring BGP routing policy, enable basic BGP functions and, make sure the following information is available.

- BGP priority value
- LOCAL_PREF value
- MED value

**Configuring BGP Route Attributes**

BGP possesses many route attributes for you to control BGP routing policies. Follow the steps in Table 260 to configure BGP route attributes:

**Table 259 Configuring BGP Route Dampening**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure BGP route dampening-related parameters</td>
<td>dampening [ half-life-reachable half-life-unreachable reuse suppress ceiling ] [ route-policy route-policy-name ]</td>
<td>Optional Not configured by default. The defaults are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- half-life-reachable: 15 (in minutes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- half-life-unreachable: 15 (in minutes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- reuse: 750</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- suppress: 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ceiling: 16000</td>
</tr>
</tbody>
</table>

**Table 260 Configuring BGP Route Attributes**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the management preference of the exterior, interior and local routes</td>
<td>preference ebgp-value ibgp-value local-value</td>
<td>Optional By default, the management preference of the exterior, interior and local routes is 256, 256, and 130.</td>
</tr>
<tr>
<td>Set the default local preference</td>
<td>default local-preference</td>
<td>Optional By default, the local preference defaults to 100.</td>
</tr>
<tr>
<td>Configure the MED attribute:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Configure the default local MED value</td>
<td>default med med-value</td>
<td>Optional By default, the med-value argument is 0.</td>
</tr>
<tr>
<td>2 Permit to compare the MED values of the routes coming from the neighbor routers in different ASs.</td>
<td>compare-different-as-med</td>
<td>Optional By default, the compare of MED values of the routes coming from the neighbor routers in different ASs is disabled.</td>
</tr>
</tbody>
</table>
Caution:

- **Using routing policy**, you can configure the preference for the routes that match the filtering conditions. As for the unmatched routes, the default preference is adopted.
- **If other conditions are the same**, the route with the lowest MED value is preferred to be the exterior route of the AS.
- **Normally**, a BGP router checks the AS_PATH attribute of the routes it receives. The routes with their AS-Path attribute containing the local AS number are ignored to avoid route loops.
- **You can configure virtual AS numbers as needed**. Virtual AS number only applies to EBGP peers. It conceals the actual local AS number. With a virtual AS number configured in an AS, only the virtual AS number is visible to EBGP peers in other ASs.
- **Use the command** that changing the AS number in the AS_PATH attribute in specific network only. Improper configuration causes route loops.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the local address as the next hop address when a BGP router advertises a route.</td>
<td><code>peer group-name next-hop-local</code></td>
<td>Required&lt;br&gt;In some network, to ensure an IBGP neighbor locates the correct next hop, you can configure the next hop address of a route to be the local address for a BGP router to advertise route information to IBGP peer groups.</td>
</tr>
<tr>
<td>Configure the AS_PATH attribute:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Configure the number of local AS number occurrences allowed</td>
<td>`peer { group-name</td>
<td>ip-address } allow-as-loop [ number ]`</td>
</tr>
<tr>
<td>2. Assign an AS number for a peer group</td>
<td><code>peer group-name as-number</code></td>
<td>Optional&lt;br&gt;By default, the local AS number is not assigned to a peer group.</td>
</tr>
<tr>
<td>3. Configure that the BGP update packets only carry the public AS number in the AS_PATH attribute when a peer sends BGP update packets to BGP peers.</td>
<td><code>peer group-name public-as-only</code></td>
<td>Optional&lt;br&gt;By default, a BGP update packet carries the private AS number.</td>
</tr>
</tbody>
</table>

Tuning and optimizing BGP network involves the following steps:

1. **BGP clock**

   BGP peers send Keepalive messages to each other periodically through the connections between them to make sure the connections operate properly. If a
router does not receive the Keepalive or any other message from its peer in a specific period (known as Holdtime), the router considers the BGP connection operates improperly and thus disconnects the BGP connection.

When establishing a BGP connection, the two routers negotiate for the Holdtime by comparing their Holdtime values and take the smaller one as the Holdtime.

2 Limiting the number of route prefixes that can be learned from a peer/peer group

By limiting the number of route prefixes that can be learned from peer/peer group to reduce the size of the local routing table, you can optimize the performance of the local router system and protect the local router.

With this function enabled on a router, when the number of route prefixes learned from a peer/peer group exceeds the configured value, the router automatically disconnects from the peer/peer group.

3 BGP connection reset

To make a new BGP routing policy taking effect, you need to reset the BGP connection. This temporarily disconnects the BGP connection. The switches support the BGP route-refresh function. With route-refresh function enabled on all the routers, if BGP routing policy changes, the local router sends refresh messages to its peers. And the peers receiving the message in turn send their routing information to the local router. Therefore, the local router can perform dynamic route update and apply the new policy without tearing down BGP connections.

If a router not supporting route-refresh exists in the network, you can only reset BGP connections with the refresh bgp command, resulting in temporary BGP disconnections.

4 BGP authentication

BGP uses TCP as the transport layer protocol. To improve the security of BGP connections, you can specify to perform MD5 authentication when a TCP connection is established. Note that the MD5 authentication of BGP does not authenticate the BGP packets. It only configures the MD5 authentication password for TCP connection, and the authentication is performed by TCP. If authentication fails, the TCP connection cannot be established.

Configuration Prerequisites

Before adjusting the BGP clock, enable basic BGP functions.

Before configuring BGP clock and authentication, make sure the following information is available.

- Value of BGP timer
- Interval for sending the update packets
- MD5 authentication password
Follow the steps in Table 261 to tune and optimize a BGP network:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td><strong>bgp as-number</strong></td>
<td>—</td>
</tr>
<tr>
<td>Configure BGP timer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Configure the Keepalive time and Holdtime of BGP.</td>
<td><strong>timer keepalive</strong>&lt;br&gt;keepalive-interval hold&lt;br&gt;holdtime-interval</td>
</tr>
<tr>
<td>2</td>
<td>Configure the Keepalive time and holdtime of a specified peer/peer group.</td>
<td><strong>peer</strong>&lt;br&gt;{(group-name</td>
</tr>
<tr>
<td></td>
<td>Configure the interval at which a peer group sends the same route update packet</td>
<td><strong>peer</strong> group-name route-update-interval seconds</td>
</tr>
<tr>
<td></td>
<td>Configure the number of route prefixes that can be learned from a BGP peer/peer group</td>
<td><strong>peer</strong>&lt;br&gt;{(group-name</td>
</tr>
<tr>
<td>Perform a soft refresh of the BGP connection manually</td>
<td><strong>return</strong></td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Perform a soft refresh of the BGP connection</td>
<td><strong>refresh bgp</strong>&lt;br&gt;{(all</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>bgp as-number</strong></td>
</tr>
<tr>
<td>Configure BGP to perform MD5 authentication when establishing TCP connection</td>
<td><strong>peer</strong>&lt;br&gt;{(group-name</td>
<td>ip-address) password **&lt;br&gt;cipher</td>
</tr>
</tbody>
</table>

**Caution:**

- The reasonable maximum interval for sending Keepalive message is one third of the Holdtime, and the interval cannot be less than 1 second, therefore, if the Holdtime is not 0, it must be 3 seconds at least.
- BGP soft reset can refresh the BGP routing table and apply a new routing policy without breaking the BGP connections.
- BGP soft reset requires all BGP routers in a network support the route-refresh function. If there is a router not supporting the route-refresh function, you need to configure the peer keep-all-routes command to save all the initial routing information of peers for the use of BGP soft reset.
**Configuring a Large-Scale BGP Network**

In large-scale network, there are large quantities of peers. Configuring and maintaining the peer becomes a big problem. Using peer group can ease the management and improve the routes sending efficiency. According to the different ASs where peers reside, the peer groups fall into IBGP peer groups and EBG peer groups. For the EBG peer group, it can also be divided into pure EBG peer group and hybrid EBG peer group according to whether the peers in the EBG group belong to the same exterior AS or not.

Community can also be used to ease the routing policy management. And its management range is much wider than that of the peer group. It is AS-independent. It controls the routing policy of multiple BGP routers.

In an AS, to ensure the connectivity among IBGP peers, you need to set up full connection among them. When there are too many IBGP peers, it will cost a lot in establishing a full connection network. Using RR or confederation can solve the problem. In a large AS, RR and confederation can be used simultaneously.

**Configuration Prerequisites**

Before configuring a large-scale BGP network, ensure network layer connectivity between adjacent nodes.

Before configuring a large-scale BGP network, you need to prepare the following data:

- Peer group type, name, and the peers included.
- If you want to use community, the name of the applied routing policy is needed.
- If you want to use RR, you need to determine the roles (client, non-client) of routers.
- If you want to use confederation, you need to determine the confederation ID and the sub-AS number.

**Configuring BGP Peer Group**

Follow the steps in Table 262 to configure a BGP peer group:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Create an IBGP peer group</td>
<td>group group-name [internal]</td>
<td>Optional</td>
</tr>
<tr>
<td>1 Create an IBGP peer group</td>
<td>peer ip-address group group-name [as-number as-number]</td>
<td>If the command is executed without the internal or external keyword, an IBGP peer group will be created. You can add multiple peers to the group, and the system will automatically create a peer in BGP view, and configure its AS number as the local AS number.</td>
</tr>
</tbody>
</table>
Table 262 Configuring BGP Peer Group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an EBGP peer group:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Create an EBGP peer group</td>
<td><code>group group-name external</code></td>
<td>Optional</td>
</tr>
<tr>
<td>2 Configure the AS number of a peer group</td>
<td><code>peer group-name as-number as-number</code></td>
<td>You can add multiple peers to the group. The system automatically creates the peer in BGP view and specifies its AS number as the one of the peer group.</td>
</tr>
<tr>
<td>3 Add a peer to a peer group</td>
<td><code>peer ip-address group group-name [ as-number as-number ]</code></td>
<td></td>
</tr>
<tr>
<td>Create a hybrid EBGP peer group:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Create an EBGP peer group</td>
<td><code>group group-name external</code></td>
<td>Optional</td>
</tr>
<tr>
<td>2 Add a peer to a peer group</td>
<td><code>peer ip-address group group-name [ as-number as-number ]</code></td>
<td>You can add multiple peers to the peer group.</td>
</tr>
<tr>
<td>Finish the session with the specified peer/peer group</td>
<td>`peer (group-name</td>
<td>ip-address ) shutdown`</td>
</tr>
</tbody>
</table>

Caution:
- It is not required to specify an AS number for creating an IBGP peer group.
- If there already exists a peer in a peer group, you can neither change the AS number of the peer group, nor delete a specified AS number through the undo command.
- In a hybrid EBGP peer group, you need to specify the AS number for all peers respectively.

Configuring BGP Community

Follow the steps in Table 263 to configure BGP community:

Table 263 Configuring BGP Community

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td><code>bgp as-number</code></td>
<td>—</td>
</tr>
<tr>
<td>Configure the peers to advertise COMMUNITY attribute to each other</td>
<td><code>peer group-name advertise-community</code></td>
<td>Required</td>
</tr>
<tr>
<td>Specify routing policy for the routes exported to the peer group</td>
<td><code>peer group-name route-policy route-policy-name export</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

Caution: When configuring BGP community, you must use a routing policy to define the specific COMMUNITY attribute, and then apply the routing policy when a peer sends routing information. For configuration of routing policy, refer to “Routing Policy Configuration” on page 371.
CHAPTER 31: BGP CONFIGURATION

Configuring BGP RR

Follow the steps in Table 264 to configure BGP RR:

Table 264 Configuring BGP RR

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure the RR and its client</td>
<td>peer group-name reflect-client</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no RR and its client is configured.</td>
</tr>
<tr>
<td>Configure route reflection between clients</td>
<td>reflect between-clients</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, route reflection is enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>between clients.</td>
</tr>
<tr>
<td>Configure cluster ID of an RR</td>
<td>reflector cluster-id</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>cluster-id</td>
<td>By default, an RR uses its own router ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>as the cluster ID.</td>
</tr>
</tbody>
</table>

Caution:

- Normally, full connection is not required between an RR and a client. A route is reflected by an RR from a client to another client. If an RR and a client are fully connected, you can disable the reflection between clients to reduce the cost.

- Normally, there is only one RR in a cluster. In this case, the router ID of the RR is used to identify the cluster. Configuring multiple RRs can improve the network stability. If there are multiple RRs in a cluster, use related command to configure the same cluster ID for them to avoid routing loopback.

Configuring BGP Confederation

Follow the steps in Table 265 to configure a BGP confederation:

Table 265 Configuring BGP Confederation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure a confederation ID</td>
<td>confederation id as-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not configured by default.</td>
</tr>
<tr>
<td>Configure the sub-ASs to be included in the confederation</td>
<td>confederation peer-as as-number&amp;&lt;1-32&gt;</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not configured by default.</td>
</tr>
<tr>
<td>Configure the compatibility of a confederation</td>
<td>confederation nonstandard</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the confederation configured is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>consistent with the RFC1965.</td>
</tr>
</tbody>
</table>

Caution:

- A confederation can include up to 32 sub-ASs. The AS number used by a sub-AS which is configured to belong to a confederation is only valid inside the confederation.

- If the confederation implementation mechanism of other routers is different from the RFC standardization, you can configure related command to make the confederation compatible with the non-standard routers.
Follow the steps in Table 266 to display the BGP configuration.

Table 266  Displaying BGP Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about peer group</td>
<td><code>display bgp [multicast] group [group-name]</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display routing information exported by BGP</td>
<td><code>display bgp [multicast] network</code></td>
<td></td>
</tr>
<tr>
<td>Display information about AS path</td>
<td><code>display bgp paths [as-regular-expression]</code></td>
<td></td>
</tr>
<tr>
<td>Display information about a BGP peer</td>
<td>`display bgp [multicast] peer [ip-address</td>
<td>verbose]</td>
</tr>
<tr>
<td>Display information in the BGP routing table</td>
<td><code>display bgp [multicast] routing [ip-address [mask]]</code></td>
<td></td>
</tr>
<tr>
<td>Display the route matching with the specific AS path ACL.</td>
<td><code>display bgp [multicast] routing as-path-acl acl-number</code></td>
<td></td>
</tr>
<tr>
<td>Display routing information about CIDR</td>
<td><code>display bgp [multicast] routing cidr</code></td>
<td></td>
</tr>
<tr>
<td>Display the route matching with the specific BGP community ACL.</td>
<td><code>display bgp [multicast] routing community-list community-list-number [whole-match]</code></td>
<td></td>
</tr>
<tr>
<td>Display information about BGP route dampening</td>
<td><code>display bgp routing dampened</code></td>
<td></td>
</tr>
<tr>
<td>Display routes with different source ASs</td>
<td><code>display bgp [multicast] routing different-origin-as</code></td>
<td></td>
</tr>
<tr>
<td>Display routing information sent to or received from a specific BGP peer</td>
<td>`display bgp [multicast] routing peer ip-address [advertised</td>
<td>received</td>
</tr>
<tr>
<td>Display routing information matching with the AS regular expression</td>
<td><code>display bgp [multicast] routing peer ip-address regular-expression as-regular-expression</code></td>
<td></td>
</tr>
<tr>
<td>Display routing statistics of BGP</td>
<td><code>display bgp [multicast] routing statistic</code></td>
<td></td>
</tr>
</tbody>
</table>
Resetting BGP Connections

To validate any BGP routing policy or protocol configuration by resetting one or more BGP connections, perform the following commands.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset all BGP connections</td>
<td>reset bgp all</td>
<td>Available in user view</td>
</tr>
<tr>
<td>Reset the BGP connection with a specified peer</td>
<td>reset bgp ip-address [ flap-info ]</td>
<td></td>
</tr>
<tr>
<td>Reset the BGP connection with a specified peer group</td>
<td>reset bgp group group-name</td>
<td></td>
</tr>
</tbody>
</table>

Clearing BGP Information

Follow the steps in Table 268 to clear the BGP information.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear the route dampening information and release the suppressed routes</td>
<td>reset bgp dampening [ network-address [ mask ] ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

BGP Configuration Examples

Configuring BGP Confederation Attribute

Network requirements

BGP runs in a large AS of a company. As the number of IBGP peers increases rapidly in the AS, more network resources for BGP communication are occupied. The customer hopes to reduce IBGP peers to minimize the CPU and network resources consumption by BGP without affecting device performance.

Based on user requirements, configure a BGP confederation to achieve the goal.

Network diagram

Figure 105 shows the network diagram.

Figure 105  Network diagram for AS confederation configuration
Table 269  Network Diagram Description

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int 10</td>
<td>172.68.10.1/24</td>
<td>100</td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int 10</td>
<td>172.68.10.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int 10</td>
<td>172.68.10.3/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 20</td>
<td>172.68.1.1/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 30</td>
<td>156.10.1.1/24</td>
<td></td>
</tr>
<tr>
<td>Switch D</td>
<td>Vlan-int 20</td>
<td>172.68.1.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch E</td>
<td>Vlan-int 30</td>
<td>156.10.1.2/24</td>
<td>200</td>
</tr>
</tbody>
</table>

Configuration plan

■ Split AS 100 into three sub-ASs: AS 1001, AS 1002, and AS 1003.
■ Run EBGP between AS 1001, AS 1002, and AS 1003.
■ AS 1001, AS 1002, and AS 1003 are each fully meshed by running IBGP.
■ Run EBGP between AS 100 and AS 200.

Configuration procedure

# Configure Switch A.

```plaintext
<SwitchA> system-view
[SwitchA] bgp 1001
[SwitchA-bgp] confederation id 100
[SwitchA-bgp] confederation peer-as 1002 1003
[SwitchA-bgp] group confed1002 external
[SwitchA-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchA-bgp] group confed1003 external
[SwitchA-bgp] peer 172.68.10.3 group confed1003 as-number 1003
```

# Configure Switch B.

```plaintext
<SwitchB> system-view
[SwitchB] bgp 1002
[SwitchB-bgp] confederation id 100
[SwitchB-bgp] confederation peer-as 1001 1003
[SwitchB-bgp] group confed1001 external
[SwitchB-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchB-bgp] group confed1003 external
[SwitchB-bgp] peer 172.68.10.3 group confed1003 as-number 1003
```

# Configure Switch C.

```plaintext
<SwitchC> system-view
[SwitchC] bgp 1003
[SwitchC-bgp] confederation id 100
[SwitchC-bgp] confederation peer-as 1001 1002
[SwitchC-bgp] group confed1001 external
[SwitchC-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchC-bgp] group confed1002 external
[SwitchC-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchC-bgp] group ebgp200 external
```
### Configuring BGP RR

#### Network requirements

BGP runs in a large AS of a company. As the number of IBGP peers increases rapidly in the AS, more network resources for BGP communication are occupied. The customer hopes to reduce IBGP peers to minimize the CPU and network resources consumption by BGP without affecting device performance. In addition, IBGP peers are partially interconnected in the AS.

Based on the requirements and networking environment, configure a BGP route reflector to achieve the goal.

#### Network diagram

Figure 106 shows the network diagram.

![Network diagram](image)

**Figure 106** Network diagram for BGP RR configuration

#### Table 270 Network diagram description

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int 100</td>
<td>1.1.1.1/8</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Vlan-int 2</td>
<td>192.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int 2</td>
<td>192.1.1.2/24</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>Vlan-int 3</td>
<td>193.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int 3</td>
<td>193.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 4</td>
<td>194.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>Switch D</td>
<td>Vlan-int 4</td>
<td>194.1.1.2/24</td>
<td></td>
</tr>
</tbody>
</table>

#### Configuration plan

- Run EBGP between the peers in AS 100 and AS 200. Inject network 1.0.0.0/8.
- Run IBGP between the peers in AS 200. Configure a star topology for the AS. Specify the central device as a route reflector and other devices as clients.
Configuration procedure

1 Configure Switch A.

<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 1.1.1.1 255.0.0.0
[SwitchA-Vlan-interface100] quit
[SwitchA] bgp 100
[SwitchA-bgp] group ex external
[SwitchA-bgp] peer 192.1.1.2 group ex as-number 200
[SwitchA-bgp] network 1.0.0.0 255.0.0.0

2 Configure Switch B.

# Configure VLAN interface IP addresses.

<SwitchB> system-view
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] interface Vlan-interface 3
[SwitchB-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[SwitchB-Vlan-interface3] quit

# Configure a BGP peer.

[SwitchB] bgp 200
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 193.1.1.1 group in

3 Configure Switch C.

# Configure VLAN interface IP addresses.

<SwitchC> system-view
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
[SwitchC-Vlan-interface3] quit
[SwitchC] interface Vlan-interface 4
[SwitchC-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[SwitchC-Vlan-interface4] quit

# Configure BGP peers and RR.

[SwitchC] bgp 200
[SwitchC-bgp] group rr internal
[SwitchC-bgp] peer rr reflect-client
[SwitchC-bgp] peer 193.1.1.2 group rr
[SwitchC-bgp] peer 194.1.1.2 group rr

4 Configure Switch D.

# Configure VLAN interface IP address.
<SwitchD> system-view
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[SwitchD-Vlan-interface4] quit

# Configure a BGP peer.

[SwitchD] bgp 200
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 194.1.1.1 group in

Use the display bgp routing command to display the BGP routing table on Switch B. Note that, Switch B has already known the existence of network 1.0.0.0.

Use the display bgp routing command to display the BGP routing table on Switch D. Note that, Switch D knows the existence of network 1.0.0.0, too.

### Configuring BGP Path Selection

#### Network requirements

A network consists of two ASs, which run BGP to communicate with each other. OSPF runs in one of them.

The requirement is to control the data forwarding path from AS 200 to AS 100.

The following gives two plans to meet the requirement:

- Use the MED attribute to control the forwarding path for packets from AS 200 to AS 100.
- Use the LOCAL_PREF attribute to control the forwarding path for packets from AS 200 to AS 100.

#### Network diagram

Figure 107 shows the network diagram.

**Figure 107** Network diagram for BGP path selection
**Configuration plan**

- Run EBGP between AS 100 and AS 200. Inject network 1.0.0.0/8.
- Run OSPF in AS 200 to realize network interconnection.
- Run IBGP between Switch D and Switch B as well as between Switch D and Switch C.
- Apply a routing policy on Switch A to modify the MED attribute of the route to be advertised to AS 200, making the data forwarding path from Switch D to AS 100 as Switch D - Switch C - Switch A.
- Apply a routing policy on Switch C to modify the LOCAL_PREF attribute of the route to be advertised to Switch D, making the data forwarding path from AS 200 to AS 100 as Switch D - Switch C - Switch A.

**Configuration procedure**

1. Configure Switch A.

```
# Configure VLAN interface IP addresses.

<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] interface Vlan-interface 3
[SwitchA-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
[SwitchA-Vlan-interface3] quit

# Enable BGP.

[SwitchA] bgp 100

# Inject network 1.0.0.0/8.

[SwitchA-bgp] network 1.0.0.0

# Configure BGP peers.

[SwitchA-bgp] group ex192 external
[SwitchA-bgp] peer 192.1.1.2 group ex192 as-number 200
```

### Table 271  Network diagram description

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int 101</td>
<td>1.1.1.1/8</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Vlan-int 2</td>
<td>192.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 3</td>
<td>193.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int 2</td>
<td>192.1.1.2/24</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>Vlan-int 4</td>
<td>194.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int 3</td>
<td>193.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 5</td>
<td>195.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>Switch D</td>
<td>Vlan-int 4</td>
<td>194.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int 5</td>
<td>195.1.1.1/24</td>
<td></td>
</tr>
</tbody>
</table>
[SwitchA-bgp] group ex193 external
[SwitchA-bgp] peer 193.1.1.2 group ex193 as-number 200
[SwitchA-bgp] quit

# Define ACL 2000 to permit the route 1.0.0.0/8.

[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule deny source any
[SwitchA-acl-basic-2000] quit

# Create a routing policy named apply_med_50, and specify node 10 with the
# permit matching mode for the routing policy. Set the MED value of the route
# matching ACL 2000 to 50.

[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit

# Create a routing policy named apply_med_100, and specify node 10 with the
# permit matching mode for the routing policy. Set the MED value of the route
# matching ACL 2000 to 100.

[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
[SwitchA-route-policy] quit

# Apply the routing policy apply_med_50 to the routing updates destined for peer
# group ex193 (the peer 193.1.1.2) and apply_med_100 to the routing updates
# destined for peer group ex192 (the peer 192.1.1.2).

[SwitchA] bgp 100
[SwitchA-bgp] peer ex193 route-policy apply_med_50 export
[SwitchA-bgp] peer ex192 route-policy apply_med_100 export

2 Configure Switch B.

# Configure VLAN interface IP addresses.

<SwitchB> system-view
[SwitchB] interface vlan 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] interface Vlan-interface 4
[SwitchB-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[SwitchB-Vlan-interface4] quit

# Configure OSPF.

[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
# Enable BGP, create a peer group, and add peers to the peer group.

```
[SwitchB] bgp 200
[SwitchB-bgp] undo synchronization
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 194.1.1.1 group in
[SwitchB-bgp] peer 195.1.1.2 group in
```

3 Configure Switch C.

# Configure VLAN interface IP addresses.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[SwitchC-Vlan-interface3] quit
[SwitchC] interface Vlan-interface 5
[SwitchC-Vlan-interface5] ip address 195.1.1.2 255.255.255.0
[SwitchC-Vlan-interface5] quit
```

# Configure OSPF.

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

# Enable BGP, create a peer group, and add peers to the peer group.

```
[SwitchC] bgp 200
[SwitchC-bgp] undo synchronization
[SwitchC-bgp] group ex external
[SwitchC-bgp] peer 193.1.1.1 group ex as-number 100
[SwitchC-bgp] group in internal
[SwitchC-bgp] peer 194.1.1.1 group in
[SwitchC-bgp] peer 194.1.1.2 group in
```

4 Configure Switch D.

# Configure VLAN interface IP addresses.

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[SwitchD-Vlan-interface4] quit
[SwitchD] interface Vlan-interface 5
[SwitchD-Vlan-interface5] ip address 195.1.1.1 255.255.255.0
[SwitchD-Vlan-interface5] quit
```

# Configure OSPF.

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
```
# Enable BGP, create a peer group, and add peers to the peer group.

```plaintext
[SwitchD] bgp 200
[SwitchD-bgp] undo synchronization
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 195.1.1.2 group in
[SwitchD-bgp] peer 194.1.1.2 group in
```

- To make the configuration take effect, all BGP neighbors need to execute the `reset bgp all` command.

- After completing the above configuration, because the MED attribute value of the route 1.0.0.0 learnt by Switch C is smaller than that of the route 1.0.0.0 learnt by Switch B, Switch D will choose the route 1.0.0.0 coming from Switch C.

- If you do not configure MED attribute of Switch A when you configure Switch A, but configure the local preference on Switch C as following:

```plaintext
# Define ACL 2000 to permit the route 1.0.0.0/8.

[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] rule deny source any
[SwitchC-acl-basic-2000] quit
```

```plaintext
# Create a routing policy named localpref, and specify node 10 with the permit matching mode for the routing policy. Set the local preference value of the route matching ACL 2000 to 200

[SwitchC] route-policy localpref permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
```

```plaintext
# Create a routing policy named localpref, and specify node 20 with the permit matching mode for the routing policy. Set the local preference value of the route to 100.

[SwitchC] route-policy localpref permit node 20
[SwitchC-route-policy] apply local-preference 100
[SwitchC-route-policy] quit
```

```plaintext
# Apply the routing policy localpref to the routing information from the peer 193.1.1.1.

[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
```

In this case, because the LOCAL_PREF value of the route 1.0.0.0 learnt by Switch C is 200, which is greater than that of the route 1.0.0.0 learnt by Switch B (Switch B does not configure the LOCAL_PREF attribute, the default value is 100), Switch D still chooses the route 1.0.0.0 coming from Switch C first.
### Troubleshooting BGP Configuration

<table>
<thead>
<tr>
<th>BGP Peer Connection Establishment Error</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When you use the <code>display bgp peer</code> command to display the BGP peer information, the connection with the opposite peer cannot be established.</td>
</tr>
</tbody>
</table>

**Analysis**

To establish a BGP peering relationship:

- Both ends need to use the 179 port to establish TCP sessions.
- Both ends need to exchange Open messages correctly.

**Troubleshooting**

1. Use the `display current-configuration` command to check the AS number configuration of the neighbor.
2. Use the `display bgp peer` command to check the IP address of the neighbor.
3. If a loopback interface is used, check whether the `peer connect-interface` command is configured.
4. If the neighbor is not physically directed, check whether the `peer ebgp-max-hop` command is configured.
5. Check whether there is an available route of the neighbor in the routing table.
6. Use the `ping -a ip-address` command to check the TCP connection.
7. Check whether you have disabled the ACL of TCP port 179.
The term router in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

IP Routing Policy
Overview

Introduction to IP Routing Policy
Routing policy is technology used to modify routing information to control the forwarding path of data packets. Routing policy is implemented by changing the route attributes such as reachability.

When a router distributes or receives routing information, it may need to implement some policies to filter the routing information, so as to receive or distribute only the routing information meeting given conditions. A routing protocol (RIP, for example) may need to import the routing information discovered by other protocols to enrich its routing knowledge. While importing routing information from another protocol, it possibly only needs to import the routes meeting given conditions and control some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a routing policy, you need to define a set of matching rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policies to advertise, receive, and import routes.

Filters
A routing protocol can reference an ACL, IP-prefix, as path, community list, or routing policy to filter routing information. The following sections describe these filters.

ACL
You can specify a range of IP addresses or subnets when defining an ACL so as to match the destination network addresses or next-hop addresses in routing information. You can reference an ACL into a routing policy to filter routing information. See “ACL Configuration” on page 663

IP-prefix list
IP-prefix list plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When IP-prefix list is applied to filter routing information, its matching object is the destination address field in routing information. Moreover, with IP-prefix list, you can use the gateway option to specify that only routing information advertised by certain routers will be received.
An IP-prefix list is identified by its IP-prefix name. Each IP-prefix list can contain multiple entries, and each entry, identified by an index-number, can independently specify the match range in the network prefix form. An index-number specifies the matching sequence in the IP-prefix list.

There is an OR relationship between entries. During the matching, the router checks entries identified by index-number in ascending order. Once an entry is matched, the IP-prefix list filtering is passed and no other entries will be checked.

**As-path**

As-path is an access control list of autonomous system path. It is only used in BGP to define the matching conditions about AS path. An as-path contains a series of AS paths which are the records of routing information passed paths during BGP routing information exchange.

**Community-list**

Community-list is only used to define the matching conditions about COMMUNITY attributes in BGP. A BGP routing information packet contains a COMMUNITY attribute field used to identify a community.

**Routing policy**

A routing policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A routing policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in ascending order of their node numbers. Each node comprises a set of if-match and apply clauses. The if-match clauses define the matching rules. The matching objects are some attributes of routing information. The relationship among the if-match clauses for a node is AND. As a result, a matching test against a node is successful only when all the matching conditions specified by the if-match clauses in the node are satisfied. The apply clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

There is an OR relationship between different nodes in a routing policy. As a result, the system examines the nodes in the routing policy in sequence, and once the route matches a node in the routing policy, it will pass the matching test of the routing policy without entering the test of the next node.

### Table 272  IP routing policy configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing policy configuration</td>
<td>Defining a routing policy</td>
<td>“Defining a Routing Policy” on page 371</td>
</tr>
<tr>
<td></td>
<td>Defining if-match clauses and apply clauses</td>
<td>“Defining if-match Clauses and apply Clauses” on page 372</td>
</tr>
<tr>
<td>IP-prefix configuration</td>
<td>Required</td>
<td>“IP-Prefix Configuration” on page 374</td>
</tr>
</tbody>
</table>

---

**IP Routing Policy Configuration Tasks**
Routing Policy Configuration

A routing policy is used to match given routing information or some attributes of routing information and change the attributes of the routing information if the conditions are met. The above-mentioned filtering lists can serve as the match conditions:

A routing policy can comprise multiple nodes and each node comprises:

- **if-match** clause: Defines matching rules; that is, the filtering conditions that the routing information should satisfy for passing the current routing policy. The matching objects are some attributes of the routing information.

- **apply** clause: Specifies actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the if-match clause. Thereby, some attributes of the route can be modified.

Configuration Prerequisites

Before configuring a routing policy, perform the following tasks:

- Configuring a filtering list,
- Configuring a routing protocol

Prepare the following data before the configuration:

- Routing policy name and node number
- Match conditions
- Route attributes to be changed

Defining a Routing Policy

<table>
<thead>
<tr>
<th>Table 273  Define a routing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Define a routing policy and enter the routing policy view</td>
</tr>
</tbody>
</table>

- **The permit** argument specifies the matching mode for a defined node in the routing policy to be in **permit** mode. If a route matches the rules for the node, the apply clauses for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.

- **The deny** argument specifies the matching mode for a defined node in the routing policy to be in **deny** mode. In this mode, no apply clause is executed. If a route satisfies all the if-match clauses of the node, no apply clause for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.

- If multiple nodes are defined in a routing policy, at least one of them should be in **permit** mode. When a routing policy is applied to filtering routing information, if a piece of routing information does not match any node, the routing information will be denied by the routing policy. If all the nodes in the routing policy are in **deny** mode, all routing information will be denied by the routing policy.
### Defining if-match Clauses and apply Clauses

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter the route-policy view</td>
<td>route-policy route-policy-name { permit</td>
<td>deny } node node-number</td>
</tr>
<tr>
<td>Define a rule to match AS path of BGP routing information</td>
<td>if-match as-path as-path-number</td>
<td>Optional</td>
</tr>
<tr>
<td>Define a rule to match COMMUNITY attributes of BGP routing information</td>
<td>if-match community { basic-community-number</td>
<td>whole-match</td>
</tr>
<tr>
<td>Define a rule to match the IP address of routing information</td>
<td>if-match { acl acl-number</td>
<td>ip-prefix ip-prefix-name }</td>
</tr>
<tr>
<td>Define a rule to match the cost of routes</td>
<td>if-match cost value</td>
<td>Optional</td>
</tr>
<tr>
<td>Define a rule to match the next-hop interface of routing information</td>
<td>if-match interface interface-type interface-number</td>
<td>Optional</td>
</tr>
<tr>
<td>Define a rule to match the next-hop address of routing information</td>
<td>if-match ip next-hop { acl acl-number</td>
<td>ip-prefix ip-prefix-name }</td>
</tr>
<tr>
<td>Add specified AS number for as-path in BGP routing information</td>
<td>apply as-path as-number&amp;&lt;1-10&gt;</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure COMMUNITY attributes for BGP routing information</td>
<td>apply community { as:nn&amp;&lt;1-13&gt;</td>
<td>no-export-subconfed</td>
</tr>
<tr>
<td>Set next hop IP address for routing information</td>
<td>apply ip next-hop ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td>Set local preference of BGP routing information</td>
<td>apply local-preference local-preference</td>
<td>Optional</td>
</tr>
<tr>
<td>Define a rule to match the tag field of OSPF routing information</td>
<td>if-match tag value</td>
<td>Optional</td>
</tr>
<tr>
<td>Apply a cost to routes satisfying matching rules</td>
<td>apply cost value</td>
<td>Optional</td>
</tr>
<tr>
<td>Set route cost type for routing information</td>
<td>apply cost-type [ internal</td>
<td>external ]</td>
</tr>
<tr>
<td>Set route source of BGP routing information</td>
<td>apply origin { igp</td>
<td>egp as-number</td>
</tr>
</tbody>
</table>
A routing policy comprises multiple nodes. There is an OR relationship between the nodes in a routing policy. As a result, the system examines the nodes in sequence, and once the route matches a node in the routing policy, it will pass the matching test of the routing policy without entering the test of the next node.

During the matching, there is an AND relationship between the if-match clauses for a routing policy node. That is, a matching test against a node is successful only when all the matching conditions specified by the if-match clauses in the node are satisfied.

If no if-match clauses are specified, all the routes will filter through the node.

A node can comprise no if-match clause or multiple if-match clauses.

Each node comprises a set of if-match and apply clauses. If-match clauses define matching rules. Apply clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

### AS Path List Configuration

This section applies to the Switch 5500G only (not the Switch 5500)

A BGP routing information packet contains an AS path field. AS path list can be used to match the AS path field in BGP routing information to filter out the routing information that does not match.

Follow the steps in Table 275 to configure an AS path list:

### Table 275  AS Path List Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Configure AS path list</td>
<td>ip as-path-acl acl-number { permit</td>
<td>deny } as-regular-expression</td>
</tr>
</tbody>
</table>

### Community List Configuration

This section applies to the Switch 5500G only (not the Switch 5500)

In BGP, COMMUNITY attributes are optional transitive. Some COMMUNITY attributes are globally recognized and they are called standard COMMUNITY attributes. Some are for special purposes and they can be customized.
A route can have one or more COMMUNITY attributes. The speaker of multiple COMMUNITY attributes of a route can act based on one, multiple or all attributes. A router can decide whether to change COMMUNITY attributes before forwarding a route to other peer entity.

Community list is used to identify community information. It falls in to two types: basic community list and advanced community list. The former one's value ranges from 1 to 99, and the latter one's ranges from 100 to 199.

Follow the steps in Table 276 to configure a community list:

Table 276  Community List Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Configure basic</td>
<td>ip community-list basic-comm-list-number [permit | deny ] ( a:a:nn &amp;(&lt;1-12&gt; ) | ) internet | no-export-subconfed | no-advertise | no-export ]*</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure advanced</td>
<td>ip community-list adv-comm-list-number [permit | deny ] comm-regular-expression</td>
<td>Optional</td>
</tr>
<tr>
<td>community list</td>
<td></td>
<td>By default, no BGP community list is defined</td>
</tr>
</tbody>
</table>

Table 277  Configure an IPv4 IP-prefix list

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>

IP-Prefix Configuration

IP-prefix plays a role similar to ACL and but is more flexible and easier to understand. When IP-prefix is applied to filtering routing information, its matching object is the destination address information field of routing information.

Configuration Prerequisites

Before configuring a filter list, prepare the following data:

- IP-prefix name
- Range of addresses to be matched

Configuring an ip-prefix list

An IP-prefix list is identified by its IP-prefix list name. Each IP-prefix list can comprise multiple entries. Each entry can independently specify a match range in the form of network prefix and is identified by an index-number. For example, the following is an IP-prefix list named abcd:

- ip ip-prefix abcd index 10 permit 1.0.0.0 8
- ip ip-prefix abcd index 20 permit 2.0.0.0 8

During the matching of a route, the router checks the entries in ascending order of index-number. Once the route matches an entry, the route passes the filtering of the IP-prefix list and no other entry will be matched.
If all the entries of the IP prefix list are in the deny mode, all routing information will be denied by the filter. In this case, you are recommended to define an entry in the permit mode with the `ip ip-prefix ip-prefix-name [index index-number] {permit | deny} network len [greater-equal greater-equal | less-equal less-equal] permit 0.0.0.0 less-equal 32` command following multiple entries in the deny mode to permit all the other IP routes.

**Displaying IP Routing Policy**

After completing the above configuration, execute the `display` command in any view to display and verify the routing policy configuration.

<table>
<thead>
<tr>
<th>Table 278</th>
<th>Display and maintain a routing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Display routing policy information</td>
<td><code>display route-policy</code></td>
</tr>
<tr>
<td>Display IP-prefix information</td>
<td><code>display ip ip-prefix</code></td>
</tr>
</tbody>
</table>

**IP Routing Policy Configuration Example**

**Configuring to Filter Received Routing Information**

**Network requirements**

Switch A communicates with Switch B. OSPF protocol is enabled on both switches. The router ID of Switch A is 1.1.1.1 and that of Switch B is 2.2.2.2.

Configure three static routes and enable OSPF on Switch A.

By configuring route filtering rules on Switch A make the three received static routes partially visible and partially shielded: the routes of network segments 20.0.0.0 and 40.0.0.0 are visible, and the route of network segment 30.0.0.0 is shielded.
Network diagram

Figure 108  Filtering received routing information

Configuration procedure

■ Configure Switch A:

# Configure the IP addresses of the interfaces.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.0.0.1 255.0.0.0
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 12.0.0.1 255.0.0.0
[SwitchA-Vlan-interface200] quit
```

# Configure three static routes.

```
[SwitchA] ip route-static 20.0.0.0 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 30.0.0.0 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 40.0.0.0 255.0.0.0 12.0.0.2
```

# Enable the OSPF protocol and specify the ID of the area to which the interface 10.0.0.1 belongs.

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

# 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
```

# Configure a routing policy.
[SwitchA] route-policy ospf permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] quit

# Apply routing policy when the static routes are imported.

[SwitchA] ospf
[SwitchA-ospf-1] import-route static route-policy ospf

■ Configure Switch B:

# Configure the IP address of the interface.

<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.0.0.2 255.0.0.0
[SwitchB-Vlan-interface100] quit

# Enable the OSPF protocol and specify the ID of the area to which the interface belongs.

[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit

■ Display the OSPF routing table on Switch B and check if routing policy takes effect.

<SwitchB> display ospf routing

OSPF Process 1 with Router ID 2.2.2.2
Routing Tables

Routing for Network
Destination         Cost Type NextHop  AdvRouter Area
10.0.0.0/8          1 Transit 10.0.0.2 1.1.1.1 0.0.0.0

Routing for ASEs
Destination         Cost Type Tag NextHop  AdvRouter
20.0.0.0/8           1 Type2   1 10.0.0.1 1.1.1.1
40.0.0.0/8           1 Type2   1 10.0.0.1 1.1.1.1

Total Nets: 3
Intra Area: 1 Inter Area: 0 ASE: 2 NSSA: 0

Network requirements
The required speed of convergence in the small network of a company is not high. The network provides two services. Main and backup links are provided for each service for the purpose of reliability. The main link of one service serves as the backup link of the other. The two services are distinguished by IP addresses. If a fault occurs to the main link of one service, dynamic backup can prevent service interruption.

Network diagram
According to the network requirements, the network topology is designed as shown in Figure 109.
Figure 109 Network diagram

**Configuration considerations**
- According to the network requirements, select RIP.
- For the OA server, the main link is between Switch A and Switch C, while the backup link is between Switch B and Switch C.
- For the service server, the main link is between Switch B and Switch C, while the backup link is between Switch A and Switch C.
- Apply a routing policy to control the cost of routes received by Switch C to provide main and backup links for the services of the OA server and service server.
**Configuration procedure**

1 Configure Switch A.

   # Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

   # Configure RIP.

   ```
   <SwitchA> system-view
   [SwitchA] rip
   [SwitchA-rip] network 1.0.0.0
   [SwitchA-rip] network 2.0.0.0
   [SwitchA-rip] network 3.0.0.0
   ```

2 Configure Switch B.

   # Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

   # Configure RIP.

   ```
   <SwitchB> system-view
   [SwitchB] rip
   [SwitchB-rip] network 1.0.0.0
   [SwitchB-rip] network 3.0.0.0
   [SwitchB-rip] network 6.0.0.0
   ```

3 Configure Switch C.

   # Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

   # Define IP-prefix 1 containing the IP address prefix 1.0.0.0/8, and IP-prefix 2 containing the IP address prefix 3.0.0.0/8.

   ```
   <SwitchC> system-view
   [SwitchC] ip ip-prefix 1 index 10 permit 1.0.0.0 8
   [SwitchC] ip ip-prefix 2 index 10 permit 3.0.0.0 8
   ```

   # Create a routing policy named in and node 10 with the matching mode being permit. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 2 and prefix list 1.

   ```
   [SwitchC-route-policy] if-match interface Vlan-interface2
   [SwitchC-route-policy] if-match ip-prefix 1
   [SwitchC-route-policy] apply cost 5
   ```

   # Create node 20 with the matching mode being permit in the routing policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 2 and prefix list 2.

   ```
   [SwitchC-route-policy] if-match interface Vlan-interface2
   [SwitchC-route-policy] if-match ip-prefix 2
   ```
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit

# Create node 30 with the matching mode being permit in the routing policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 6 and prefix list 1.

[SwitchC] route-policy in permit node 30
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 1
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit

# Create node 40 with the matching mode being permit in the routing policy. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 6 and prefix list 2.

[SwitchC] route-policy in permit node 40
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 2
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit

# Create node 50 with the matching mode being permit, to allow all routing information to pass.

[SwitchC] route-policy in permit node 50
[SwitchC-route-policy] quit

# Configure RIP and apply the routing policy in to the incoming routing information.

[SwitchC] rip
[SwitchC-rip] network 1.0.0.0
[SwitchC-rip] network 3.0.0.0
[SwitchC-rip] network 6.0.0.0
[SwitchC-rip] filter-policy route-policy in import

Configuration verification

1. Display data forwarding paths when the main link of the OA server between Switch A and Switch C works normally.

<SwitchC> display ip routing-table
Routing Table: public net
<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0/8</td>
<td>RIP</td>
<td>100</td>
<td>5</td>
<td>2.2.2.1</td>
<td>Vlan-interface2</td>
</tr>
<tr>
<td>2.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>2.2.2.2</td>
<td>Vlan-interface2</td>
</tr>
<tr>
<td>2.2.2.2/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>3.0.0.0/8</td>
<td>RIP</td>
<td>100</td>
<td>5</td>
<td>6.6.6.5</td>
<td>Vlan-interface6</td>
</tr>
<tr>
<td>6.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>6.6.6.6</td>
<td>Vlan-interface6</td>
</tr>
<tr>
<td>6.6.6.6/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>192.168.0.39</td>
<td>Vlan-interface1</td>
</tr>
<tr>
<td>192.168.0.39/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

2. Display data forwarding paths when the main link of the OA server between Switch A and Switch C is down.

```
<SwitchC> display ip routing-table
Routing Table: public net

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0/8</td>
<td>RIP</td>
<td>100</td>
<td>6</td>
<td>6.6.6.5</td>
<td>Vlan-interface2</td>
</tr>
<tr>
<td>3.0.0.0/8</td>
<td>RIP</td>
<td>100</td>
<td>5</td>
<td>6.6.6.5</td>
<td>Vlan-interface6</td>
</tr>
<tr>
<td>6.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>6.6.6.6</td>
<td>Vlan-interface6</td>
</tr>
<tr>
<td>6.6.6.6/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>192.168.0.39</td>
<td>Vlan-interface1</td>
</tr>
<tr>
<td>192.168.0.39/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

Precautions
1 When you configure the **apply cost** command in a routing policy:
   - The new cost should be greater than the original one to prevent RIP from generating routing loop in the case that a loop exists in the topology.
   - The cost will become 16 if you try to set it to a value greater than 16.
   - The cost will become the original one if you try to set it to 0.
   - The cost will still be 16 if you try to set it to 16.
2 Using the **if-match interface** command will match the routes whose outgoing interface to the next hop is the specified interface.
3 You are recommended to configure a node to match all routes not passing the preceding nodes in a routing policy.
4 If the cost of a received RIP route is equal to 16, the cost specified by the **apply cost** command in a routing policy will not be applied to the route, that is, the cost of the route is equal to 16.
5 Using the **filter-policy** command does not filter redistributed routes.

### Troubleshooting IP Routing Policy

<table>
<thead>
<tr>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>The routing policy cannot filter routing information correctly when the routing protocol runs normally.</td>
</tr>
</tbody>
</table>

**Analysis**

The routing policy cannot filter routing information correctly in the following two cases:
- All nodes in the routing policy are in the **deny** mode.
- All entries in the IP-prefix list are in the **deny** mode.

**Solution**

1 Use the **display ip ip-prefix** command to display the configuration of the IP-prefix list.
2 Use the **display route-policy** command to display the configuration of the routing policy.
The term router in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

---

**Route Capacity Configuration Overview**

**Introduction**

In practical networking applications, there are a large number of routes, especially OSPF routes and BGP routes (Switch 500G), in the routing table. Normally, routing information is stored in the memory of the switch. While the size of the routing table increases, the total memory of the switch remains unchanged unless the hardware is upgraded. However, upgrading may not always solve the problem.

To solve this problem, the Switch 5500 provides a mechanism to control the size of the routing table; that is, monitoring the free memory in the system to determine whether to add new routes to the routing table and whether to keep the connection of a routing protocol.

**CAUTION**: Normally, the default configuration of the system can meet the requirements. To avoid decreasing system stability and availability due to improper configuration, it is not recommended to modify the configuration.

**Route Capacity Limitation**

Huge routing tables are usually caused by OSPF route entries and BGP route entries. Therefore, the route capacity limitation of a switch applies only to OSPF routes and BGP routes, instead of static routes and RIP routes. The route capacity limitation is implemented by controlling the size of the free memory of the switch.

When the free memory of the switch is equal to or lower than the lower limit, OSPF or BGP connection will be disconnected and OSPF or BGP routes will be removed from the routing table.

- If automatic protocol connection recovery is enabled, when the free memory of the switch restores to a value larger than the safety value, the switch automatically re-establishes the OSPF or BGP connection.

- If the automatic protocol connection recovery function is disabled, the switch will not reestablish the disconnected OSPF or BGP connection even when the free memory restores to a value larger than the safety value.
Route capacity limitation configuration includes:

- Configuring the lower limit and the safety value of switch memory,
- Enabling/disabling the switch to recover the disconnected routing protocol automatically.

### Configuring the Lower Limit and the Safety Value of the Switch Memory

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
</tbody>
</table>
| Set the lower limit and the safety value of switch memory | memory { safety safety-value | limit limit-value }* | Optional By default
  - safety-value is 5
  - limit-value is 4 |

The safety value must be greater than the lower limit value.

### Enabling/Disabling Automatic Protocol Recovery

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enable automatic protocol recovery</td>
<td>memory auto-establish enable</td>
<td>Optional By default, automatic protocol recovery is enabled.</td>
</tr>
</tbody>
</table>

### Displaying and Maintaining Route Capacity Limitation Configuration

After completing the above configuration, you can use the display command in any view to display and verify the route capacity configuration.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display memory occupancy of a switch</td>
<td>display memory</td>
<td>You can execute the display command in any view.</td>
</tr>
<tr>
<td>Display the route capacity related memory setting and state information</td>
<td>display memory limit</td>
<td></td>
</tr>
</tbody>
</table>
In this manual, the term router refers to a router in the generic sense and a Layer 3 Ethernet switch running an IP multicast protocol.

### Multicast Overview

With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conference, online auction, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes in unicast, broadcast, and multicast.

### Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends a separate copy of the information to the user, as shown in Figure 110:

**Figure 110**  Information transmission in the unicast mode
Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need this information, the server must send many pieces of information with the same content to the users. Therefore, the limited bandwidth becomes the bottleneck in information transmission. This shows that unicast is not good for the transmission of a great deal of information.

**Information Transmission in the Broadcast Mode**

When you adopt broadcast, the system transmits information to all users on a network. Any user on the network can receive the information, no matter the information is needed or not. Figure 111 shows information transmission in broadcast mode.

*Figure 111  Information transmission in the broadcast mode*

Assume that Hosts B, D, and E need the information. The source server broadcasts this information through routers, and Hosts A and C on the network also receive this information.

As we can see from the information transmission process, the security and legal use of paid service cannot be guaranteed. In addition, when only a small number of users on the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

Therefore, broadcast is disadvantageous in transmitting data to specific users; moreover, broadcast occupies large bandwidth.

**Information Transmission in the Multicast Mode**

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast deliver a low efficiency.
Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With multicast distribution trees established for multicast data packets through multicast routing protocols, the packets are duplicated and distributed at the nearest nodes, as shown in Figure 112:

Assume that Hosts B, D and E need the information. To transmit the information to the right users, it is necessary to group Hosts B, D and E into a receiver set. The routers on the network duplicate and distribute the information based on the distribution of the receivers in this set. Finally, the information is correctly delivered to Hosts B, D, and E.

The advantages of multicast over unicast are as follows:

- No matter how many receivers exist, there is only one copy of the same multicast data flow on each link.
- With the multicast mode used to transmit information, an increase of the number of users does not add to the network burden remarkably.

The advantages of multicast over broadcast are as follows:

- A multicast data flow can be sent only to the receiver that requires the data.
- Multicast brings no waste of network resources and makes proper use of bandwidth.

**Roles in Multicast**

The following roles are involved in multicast transmission:

- An information sender is referred to as a multicast source (Source in Figure 112).
- Each receiver is a multicast group member (Receiver in Figure 112).
All receivers interested in the same information form a multicast group. Multicast groups are not subject to geographic restrictions.

A router that supports Layer 3 multicast is called multicast router or Layer 3 multicast device. In addition to providing multicast routing, a multicast router can also manage multicast group members.

For a better understanding of the multicast concept, you can assimilate multicast transmission to the transmission of TV programs, as shown in Table 283.

Table 283  An analogy between TV transmission and multicast transmission

<table>
<thead>
<tr>
<th>Step</th>
<th>TV transmission</th>
<th>Multicast transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A TV station transmits a TV program through a television channel.</td>
<td>A multicast source sends multicast data to a multicast group.</td>
</tr>
<tr>
<td>2</td>
<td>A user tunes the TV set to the channel.</td>
<td>A receiver joins the multicast group.</td>
</tr>
<tr>
<td>3</td>
<td>The user starts to watch the TV program transmitted by the TV station via the channel.</td>
<td>The receiver starts to receive the multicast data that the source sends to the multicast group.</td>
</tr>
<tr>
<td>4</td>
<td>The user turns off the TV set.</td>
<td>The receiver leaves the multicast group.</td>
</tr>
</tbody>
</table>

A multicast source does not necessarily belong to a multicast group. Namely, a multicast source is not necessarily a multicast data receiver.

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.

Advantages of multicast

Advantages of multicast include:

- Enhanced efficiency: Multicast decreases network traffic and reduces server load and CPU load.
- Optimal performance: Multicast reduces redundant traffic.
- Distributive application: Multicast makes multiple-point application possible.

Application of multicast

The multicast technology effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission, over an IP network, multicast greatly saves network bandwidth and reduces network load.

Multicast provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.
Multicast Models

Based on the multicast source processing modes, there are three multicast models:

■ Any-Source Multicast (ASM)
■ Source-Filtered Multicast (SFM)
■ Source-Specific Multicast (SSM)

ASM model

In the ASM model, any sender can become a multicast source and send information to a multicast group; 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 a multicast source in advance. However, they can join or leave the multicast group at any time.

SFM model

The SFM model is derived from the ASM model. From the view of a sender, the two models have the same multicast group membership architecture.

Functionally, the SFM model is an extension of the ASM model. In the SFM model, the upper layer software checks the source address of received multicast packets so as to permit or deny 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 means. In addition, the SSM model uses a multicast address range that is different from that of the ASM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

Multicast Architecture

The purpose of IP multicast is to transmit information from a multicast source to receivers in the multicast mode and to satisfy information requirements of receivers. You should be concerned about:

■ Host registration: What receivers reside on the network?
■ Technologies of discovering a multicast source: Which multicast source should the receivers receive information from?
■ Multicast addressing mechanism: Where should the multicast source transports information?
■ Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:
CHAPTER 34: MULTICAST OVERVIEW

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.
- Host registration: A receiving host joins and leaves a multicast group dynamically using the membership registration mechanism.
- Multicast routing: A router or switch transports packets from a multicast source to receivers by building a multicast distribution tree with multicast routes.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol suite must support the function of sending and receiving multicast information.

Multicast Address

As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

**IP multicast address**

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, there are a group of destination addresses (called group address), rather than one address. All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.
- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.

Note that:

- The IP addresses of a permanent multicast group keep unchanged, while the members of the group can be changed.
There can be any number of, or even zero, members in a permanent multicast group.

Those IP multicast addresses not assigned to permanent multicast groups can be used by temporary multicast groups.

Class D IP addresses range from 224.0.0.0 to 239.255.255.255. For details, see Table 284.

<table>
<thead>
<tr>
<th>Range and description of Class D IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class D address range</strong></td>
</tr>
<tr>
<td>224.0.0.0 to 224.0.0.255</td>
</tr>
<tr>
<td>224.0.1.0 to 231.255.255.255 and 233.0.0.0 to 238.255.255.255</td>
</tr>
<tr>
<td>232.0.0.0 to 232.255.255.255</td>
</tr>
<tr>
<td>239.0.0.0 to 239.255.255.255</td>
</tr>
</tbody>
</table>

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. The following table lists commonly used reserved IP multicast addresses:

<table>
<thead>
<tr>
<th>Reserved IP multicast addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class D address range</strong></td>
</tr>
<tr>
<td>224.0.0.1</td>
</tr>
<tr>
<td>224.0.0.2</td>
</tr>
<tr>
<td>224.0.0.3</td>
</tr>
<tr>
<td>224.0.0.4</td>
</tr>
<tr>
<td>224.0.0.5</td>
</tr>
<tr>
<td>224.0.0.6</td>
</tr>
<tr>
<td>224.0.0.7</td>
</tr>
<tr>
<td>224.0.0.8</td>
</tr>
<tr>
<td>224.0.0.9</td>
</tr>
<tr>
<td>224.0.0.11</td>
</tr>
<tr>
<td>224.0.0.12</td>
</tr>
<tr>
<td>224.0.0.13</td>
</tr>
<tr>
<td>224.0.0.14</td>
</tr>
<tr>
<td>224.0.0.15</td>
</tr>
<tr>
<td>224.0.0.16</td>
</tr>
<tr>
<td>224.0.0.17</td>
</tr>
<tr>
<td>224.0.0.18</td>
</tr>
<tr>
<td>224.0.0.19 to 224.0.0.255</td>
</tr>
</tbody>
</table>
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

**Ethernet multicast MAC address**

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0x01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 113 describes the mapping relationship:

![Multicast address mapping](image1)

The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address. Thus, five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

**Multicast Protocols**

- 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, PIM, and MSDP; 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.

- 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 114 describes where these multicast protocols are in a network.
1 Multicast management protocols

Typically, the Internet Group Management Protocol (IGMP) 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 autonomous system (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).

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 and multicast VLAN. Figure 115 shows where these protocols are in the network.

Figure 115 Positions of Layer 2 multicast protocols

1 IGMP Snooping
Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling the flooding of multicast data in a Layer 2 network.

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 the IP 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.

- In the network, multicast packet transmission is based on the guidance of the multicast forwarding table derived from the unicast routing table or the multicast routing table specially provided for multicast.
- 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.

The RPF mechanism enables multicast devices to forward multicast packets correctly based on the multicast route configuration. In addition, the RPF mechanism also helps avoid data loops caused by various reasons.
Implementation of the RPF Mechanism

Upon receiving a multicast packet that a multicast source $S$ sends to a multicast group $G$, the multicast device first searches its multicast forwarding table:

1. If the corresponding $(S, G)$ entry exists, and the interface on which the packet actually arrived is the incoming interface in the multicast forwarding table, the router forwards the packet to all the outgoing interfaces.

2. If the corresponding $(S, G)$ entry exists, but the interface on which the packet actually arrived is not the incoming interface in the multicast forwarding table, the multicast packet is subject to an RPF check.
   - If the result of the RPF check shows that the RPF interface is the incoming interface of the existing $(S, G)$ entry, this means that the $(S, G)$ entry is correct but the packet arrived from a wrong path and is to be discarded.
   - If the result of the RPF check shows that the RPF interface is not the incoming interface of the existing $(S, G)$ entry, this means that the $(S, G)$ entry is no longer valid. The router replaces the incoming interface of the $(S, G)$ entry with the interface on which the packet actually arrived and forwards the packet to all the outgoing interfaces.

3. If no corresponding $(S, G)$ entry exists in the multicast forwarding table, the packet is also subject to an RPF check. The router creates an $(S, G)$ entry based on the relevant routing information and using the RPF interface as the incoming interface, and installs the entry into the multicast forwarding table.
   - If the interface on which the packet actually arrived is the RPF interface, the RPF check is successful and the router forwards the packet to all the outgoing interfaces.
   - If the interface on which the packet actually arrived is not the RPF interface, the RPF check fails and the router discards the packet.

RPF Check

The basis for an RPF check is a unicast route. A unicast routing table contains the shortest path to each destination subnet. A multicast routing protocol does not independently maintain any type of unicast route; instead, it relies on the existing unicast routing information in creating multicast routing entries.

When performing an RPF check, a router searches its unicast routing table. The specific process is as follows: The router automatically chooses an optimal unicast route by searching its unicast routing table, using the IP address of the packet source as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.

Assume that unicast routes exist in the network, as shown in Figure 116. Multicast packets travel along the SPT from the multicast source to the receivers.
A multicast packet from Source arrives to VLAN-interface 1 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. Switch C performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is VLAN-interface 2. This means that the interface on which the packet actually arrived is not the RPF interface. The RPF check fails and the packet is discarded.

A multicast packet from Source arrives to VLAN-interface 2 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. The router performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is the interface on which the packet actually arrived. The RPF check succeeds and the packet is forwarded.
Common Multicast Configuration

Table 286  Common multicast configuration tasks

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Enabling Multicast Packet Buffering&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Enabling Multicast Routing&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring Limit on the Number of Route Entries&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Suppression on the Multicast Source Port&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Clearing Multicast Forwarding and Routing Entries&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Multicast MAC Address Entry&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Dropping Unknown Multicast Packets&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Enabling Multicast Packet Buffering

With the multicast packet buffering feature enabled, multicast packets delivered to the CPU are buffered while the corresponding multicast forwarding entries are being created and then forwarded out according to the multicast forwarding entries after entry creation.

This mechanism buffers multicast packets at the price of impact to the CPU and extra memory usage.

Table 287  Enable multicast packet buffering

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable multicast packet buffering</td>
<td>multicast storing-enable</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the maximum number of packets that can be buffered per multicast forwarding entry</td>
<td>multicast storing-packet</td>
<td>By default, this function is disabled.</td>
</tr>
<tr>
<td></td>
<td>packet-number</td>
<td>The system default is 100.</td>
</tr>
</tbody>
</table>

CAUTION: The multicast packet buffering feature should be enabled only before multicast routing is enabled.

Enabling Multicast Routing

Table 288  Enable multicast routing

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
To guard against attacks on any socket not in use, the Switch 5500 provides the following functions to achieve enhanced security:

- The system opens the RAW Socket used for multicast routing only if multicast routing is enabled.
- When you disable multicast routing, the RAW Socket used for multicast routing is also closed.

**CAUTION:** IGMP, PIM and MSDP configurations can be performed only if multicast routing is enabled.

### Configuring Limit on the Number of Route Entries

Too many multicast routing entries can exhaust the router’s memory and thus result in lower router performance. Therefore, the number of multicast routing entries should be limited.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable multicast routing</td>
<td>multicast-routing-enable</td>
<td>Required&lt;br&gt;Disabled by default.</td>
</tr>
</tbody>
</table>

### Configuring Suppression on the Multicast Source Port

Some users may deploy unauthorized multicast servers on the network. This affects the use of network bandwidth and transmission of multicast data of authorized users by taking network resources. You can configure multicast source port suppression on certain ports to prevent unauthorized multicast servers attached to these ports from sending multicast traffic to the network.

**Configuring multicast source port suppression in system view**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure multicast source port suppression</td>
<td>multicast-source-deny [ interface interface-list ]</td>
<td>Optional&lt;br&gt;Multicast source port suppression is disabled by default.</td>
</tr>
</tbody>
</table>
Configuring multicast source port suppression in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure multicast source port suppression</td>
<td>multicast-source-deny</td>
<td>Optional Multicast source port suppression is disabled by default.</td>
</tr>
</tbody>
</table>

Clearing Multicast Forwarding and Routing Entries

To release system memory, you can use reset commands to clear multicast routing entries, multicast forwarding entries, and related statistics information stored in the device.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear multicast forwarding entries and, with statistics specified, the corresponding statistics information</td>
<td>reset multicast forwarding-table</td>
<td>Use the reset commands in user view.</td>
</tr>
<tr>
<td>Clear routing entries in the core multicast routing table</td>
<td>reset multicast routing-table</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Multicast MAC Address Entry

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through a Layer 2 multicast protocol. Alternatively, you can statically bind a port to a multicast MAC address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet for a multicast group not yet registered on the switch, the switch will flood the packet within the VLAN to which the port belongs. You can configure a static multicast MAC address entry to avoid this.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a multicast MAC address entry</td>
<td>mac-address multicast interface interface-list vlan vlan-id</td>
<td>Required The mac-address argument must be a multicast MAC address.</td>
</tr>
</tbody>
</table>
CHAPTER 35: COMMON MULTICAST CONFIGURATION

If the multicast MAC address entry to be created already exists, the system gives you a prompt.

If you want to add a port to a multicast MAC address entry created through the `mac-address multicast` command, you need to remove the entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.

You cannot configure a multicast MAC address starting with 01005e on a device with IRF Fabric enabled.

You cannot enable link aggregation on a port on which you have configured a multicast MAC address, and you cannot configure a multicast MAC address on an aggregation port.

You cannot configure a multicast MAC address starting with 01005e in an IGMP-Snooping-enabled VLAN. You can do that if IGMP Snooping is not enabled in the VLAN.

### Configuring Dropping Unknown Multicast Packets

Generally, if the multicast address of the multicast packet received on the switch is not registered on the local switch, the packet will be flooded in the VLAN. When the function of dropping unknown multicast packets is enabled, the switch will drop any multicast packets whose multicast address is not registered. Thus, the bandwidth is saved and the processing efficiency of the system is improved.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure dropping unknown multicast packets</td>
<td><code>unknown-multicast drop enable</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the function of dropping unknown multicast packets is disabled.</td>
</tr>
</tbody>
</table>

### Displaying and Maintaining Common Multicast Configuration

After the above-described configuration, you can use the `display` command in any view to verify the configuration.

The information about the multicast forwarding table is mainly used for debugging. Generally, you can get the required information by checking the core multicast routing table.

Three kinds of tables affect multicast data transmission. Their correlations are as follows:
Each multicast routing protocol has its own multicast routing table, such as PIM routing table.

The information of different multicast routing protocols forms a general multicast routing table.

Consistent with the multicast routing table, the multicast forwarding table is the table that guide multicast forwarding.

### Table 296  Display common multicast configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the statistics information about multicast source port suppression</td>
<td><code>display multicast-source-deny [ interface interface-type [ interface-number ] ]</code></td>
<td>These commands can be executed in any view.</td>
</tr>
<tr>
<td>Display multicast forwarding table information containing port information</td>
<td><code>display mpm forwarding-table [ group-address ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the information about the IP multicast groups and MAC multicast groups in a VLAN or all VLANs</td>
<td><code>display mpm group [ vlan vlan-id ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the created multicast MAC table entries</td>
<td>`display mac-address multicast [ static [ { { mac-address vlan vlan-id</td>
<td>vlan vlan-id } [ count ]</td>
</tr>
</tbody>
</table>
### IGMP Overview

As a TCP/IP protocol responsible for IP multicast group member management, the Internet Group Management Protocol (IGMP) is used by IP hosts to establish and maintain their multicast group memberships to immediately neighboring multicast routers.

### IGMP Versions

So far, there are three IGMP versions:

- IGMPv1 (documented in RFC 1112)
- IGMPv2 (documented in RFC 2236)
- IGMPv3 (documented in RFC 3376)

All IGMP versions support the Any-Source Multicast (ASM) model. In addition, IGMPv3 provides strong support to the Source-Specific Multicast (SSM) model.

### Work Mechanism of IGMPv1

IGMPv1 manages multicast group memberships mainly based on the query and response mechanism.

Of multiple multicast routers on the same subnet, all the routers can hear IGMP membership report messages (often referred to as reports) from hosts, but only one router is needed for sending IGMP query messages (often referred to as queries). So, a querier election mechanism is required to determine which router will act as the IGMP querier on the subnet.

In IGMPv1, the designated router (DR) elected by a multicast routing protocol (such as PIM) serves as the IGMP querier.

For more information about a DR, refer to “DR election” on page 417.
Assume that Host B and Host C are expected to receive multicast data addressed to multicast group G1, while Host A is expected to receive multicast data addressed to G2, as shown in Figure 117. The basic process that the hosts join the multicast groups is as follows:

1. The IGMP querier (Router B in the figure) periodically multicasts IGMP queries (with the destination address of 224.0.0.1) to all hosts and routers on the local subnet.

2. Upon receiving a query message, Host B or Host C (the delay timer of whichever expires first) sends an IGMP report to the multicast group address of G1, to announce its interest in G1. Assume it is Host B that sends the report message.

3. Host C, which is on the same subnet, hears the report from Host B for joining G1. Upon hearing the report, Host C will suppress itself from sending a report message for the same multicast group, because the IGMP routers (Router A and Router B) already know that at least one host on the local subnet is interested in G1. This mechanism, known as IGMP report suppression, helps reduce traffic over the local subnet.

4. At the same time, because Host A is interested in G2, it sends a report to the multicast group address of G2.

5. Through the above-mentioned query/report process, the IGMP routers learn that members of G1 and G2 are attached to the local subnet, and generate (*, G1) and (*, G2) multicast forwarding entries, which will be the basis for subsequent multicast forwarding, where * represents any multicast source.

6. When the multicast data addressed to G1 or G2 reaches an IGMP router, because the (*, G1) and (*, G2) multicast forwarding entries exist on the IGMP router, the router forwards the multicast data to the local subnet, and then the receivers on the subnet receive the data.

As IGMPv1 does not specifically define a Leave Group message, upon leaving a multicast group, an IGMPv1 host stops sending reports with the destination
address being the address of that multicast group. If no member of a multicast
group exists on the subnet, the IGMP routers will not receive any report addressed
to that multicast group, so the routers will delete the multicast forwarding entries
corresponding to that multicast group after a period of time.

Enhancements Provided by IGMPv2

Compared with IGMPv1, IGMPv2 provides the querier election mechanism and
Leave Group mechanism.

**Querier election mechanism**

In IGMPv1, the DR elected by the Layer 3 multicast routing protocol (such as PIM)
serves as the querier among multiple routers on the same subnet.

In IGMPv2, an independent querier election mechanism is introduced. The querier
election process is as follows:

1. Initially, every IGMPv2 router assumes itself as the querier and sends IGMP general
   query messages (often referred to as general queries) to all hosts and routers on
   the local subnet (the destination address is 224.0.0.1).

2. Upon hearing a general query, every IGMPv2 router compares the source IP
   address of the query message with its own interface address. After comparison,
   the router with the lowest IP address wins the querier election and all other
   IGMPv2 routers become non-queriers.

3. All the non-queriers start a timer, known as **other querier present timer**. If a
   router receives an IGMP query from the querier before the timer expires, it resets
   this timer; otherwise, it assumes the querier to have timed out and initiates a new
   querier election process.

**Leave group mechanism**

In IGMPv1, when a host leaves a multicast group, it does not send any notification
 to the multicast router. The multicast router relies on IGMP query response timeout
 to know whether a group no longer has members. This adds to the leave latency.

In IGMPv2, on the other hand, when a host leaves a multicast group:

1. This host sends a Leave Group message (often referred to as leave message) to all
   routers (the destination address is 224.0.0.2) on the local subnet.

2. Upon receiving the leave message, the querier sends a configurable number of
   group-specific queries to the group being left. The destination address field and
   group address field of message are both filled with the address of the multicast
   group being queried.

3. One of the remaining members, if any on the subnet, of the group being queried
   should send a membership report within the maximum response time set in the
   query messages.

4. If the querier receives a membership report for the group within the maximum
   response time, it will maintain the memberships of the group; otherwise, the
   querier will assume that no hosts on the subnet are still interested in multicast
   traffic to that group and will stop maintaining the memberships of the group.
IGMP Proxy

A lot of stub networks (stub domains) are involved in the application of a multicast routing protocol (PIM-DM for example) over a large-scaled network. It is a hard work to configure and manage these stub networks.

To reduce the workload of configuration and management without affecting the multicast connection of leaf networks, you can configure an IGMP Proxy on a Layer 3 switch in the stub network (Switch B shown in Figure 118). The Layer 3 switch will then forward IGMP join or IGMP leave messages sent by the connected hosts. After IGMP Proxy is configured, the stub switch is no longer a PIM neighbor but a host for the exterior network. The Layer 3 switch receives the multicast data of corresponding groups only when it has directly attached multicast members.

Figure 118  Diagram for IGMP proxy

Figure 118 shows an IGMP Proxy diagram for a stub network. The upstream interface, VLAN-interface 1 of Switch B is the proxy interface for the downstream interface VLAN-interface 2.

Configure Switch B as follows:

Enable multicast routing, and then enable PIM and IGMP on VLAN-interface 1 and VLAN-interface 2. Run the `igmp proxy` command on VLAN-interface 1 to configure it as the proxy interface for VLAN-interface 2.

Configure Switch A as follows:

- Enable multicast routing, enable IGMP and PIM on VLAN-interface 1.
- Configure the `pim neighbor-policy` command to filter PIM neighbors in the network segment 33.33.33.0/24. That is, Switch A does not consider Switch B as its PIM neighbor.

In this case, when Switch B of the stub network receives from VLAN-interface 2 an IGMP join or IGMP leave message sent by the host, it changes the source address of the IGMP information to the address of VLAN-interface 1, 33.33.33.2, and send the information to VLAN-interface 1 of Switch A. For Switch A, this works as if there is a host directly connected to VLAN-interface 1.
Similarly, when Switch B receives the IGMP general or group-specific query message from the Layer 3 Switch A, Switch B also changes the source address of the query message to the IP address of VLAN-interface 2, 22.22.22.1, and send the message from VLAN-interface 2.

### Configuring IGMP

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling IGMP”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring IGMP Version”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring Options Related to IGMP Query Messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Maximum Allowed Number of Multicast Groups”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring a Multicast Group Filter”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring Simulated Joining”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring IGMP Proxy”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Removing Joined IGMP Groups from an Interface”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Enabling IGMP

First, IGMP must be enabled on the interface on which the multicast group memberships are to be established and maintained.

#### Table 298 Enable IGMP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enable IP multicast routing</td>
<td>multicast routing-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Enable IGMP</td>
<td>igmp enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

**CAUTION:** Before performing the following configurations described in this chapter, you must enable multicast routing and enable IGMP on the specific interfaces.

### Configuring IGMP Version

#### Table 299 Configure IGMP version

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface Vlan-interface interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure the IGMP version</td>
<td>igmp version (1</td>
<td>2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The system default is IGMP version 2.</td>
</tr>
</tbody>
</table>

**CAUTION:** IGMP versions cannot be switched to one another automatically. Therefore, all the interfaces on a subnet must be configured to use the same IGMP version.
Configuring Options Related to IGMP Query Messages

**IGMP general query**
An IGMP router sends IGMP general query messages to the local subnet periodically, and multicast receiver hosts send IGMP reports in response to IGMP queries. Thus the router learns which multicast groups on the subnet have active members.

**IGMP group-specific query**
On a multi-access network, the query router (querier for short) maintains group memberships. After the related features are configured, the IGMP querier sends a configurable number of IGMP group-specific queries at a configurable interval when it receives an IGMP leave message from the hosts.

Suppose a host in a multicast group decides to leave the multicast group. The related procedure is as follows:

- The host sends an IGMP leave message.
- When the IGMP querier receives the message, it sends robust-value IGMP group-specific query messages at the interval of lastmember-queryinterval.
- If other hosts are interested in the group after receiving the IGMP group-specific query message from the querier, they must send IGMP report messages within the maximum response time specified in the query messages.
- If the IGMP querier receives IGMP report messages from other hosts within the period of robust-value \times lastmember-queryinterval, it will maintain the membership of the group.
- If the IGMP querier does not receive IGMP report messages from other hosts after the period of robust-value \times lastmember-queryinterval, it considers that the group has no members on the local subnet and removes the forwarding table entry for the group.

You can use the `igmp max-response-time` command to set the maximum response time for general IGMP query messages, while that of an IGMP group-specific query message is determined by robust-value \times lastmember-queryinterval.

The procedure is only fit for the occasion where IGMP queriers run IGMP version 2.

**IGMP querier election**
On a subnet containing multiple IGMP-enabled interfaces, the one with the lowest IP address becomes the IGMP querier. If non-querier interfaces receive no query message within the period configured in the `igmp timer other-querier-present` command, the current IGMP querier is considered to be down. In this case, a new IGMP querier election process takes place.

**The maximum response time of IGMP general query messages**
When the host receives a general query message, it will set a timer for each of its multicast groups. The timer value is selected from 0 to the maximum response time at random. When the value of a timer decreases to 0, the host will send the membership information of the multicast group.
By configuring reasonable maximum response time, you can enable the host to respond to the query information quickly and enable the Layer 3 switch to understand the membership information of multicast groups quickly.

Table 300  Configure options related to IGMP query messages

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the query interval</td>
<td>igmp timer query seconds</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the interval of sending IGMP group-specific query messages</td>
<td>igmp lastmember-queryinterval seconds</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the number of times of sending IGMP group-specific query messages</td>
<td>igmp robust-count robust-value</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the other querier present timer</td>
<td>igmp timer other-querier-present seconds</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the maximum response time of IGMP general queries</td>
<td>igmp max-response-time seconds</td>
<td>Optional</td>
</tr>
</tbody>
</table>

By configuring the maximum number of IGMP multicast groups allowed to be joined on an interface of the switch, you can control the number of programs on demand available for users attached to the interface, thus to control the bandwidth usage on the interface.

Table 301  Configure the maximum number of multicast groups allowed on an interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the maximum number of multicast groups allowed on the interface</td>
<td>igmp group-limit limit</td>
<td>Required</td>
</tr>
</tbody>
</table>

**CAUTION:**

- After the maximum number of multicast groups is reached, the interface will not join any new multicast group.
- If you configure the maximum number of multicast groups allowed on the interface to 1, a new group registered on the interface supersedes the existing one automatically.
- If the number of existing multicast groups is larger than the configured limit on the number of joined multicast groups on the interface, the device will remove...
CHAPTER 36: IGMP CONFIGURATION

Configuring a Multicast Group Filter

A multicast router determines the group memberships in the specified subnet by analyzing the received IGMP reports. To restrict the hosts on the network attached to an interface from joining certain multicast groups, you can apply an ACL rule on the interface as a group filter that limits the range of multicast groups that the interface serves. You can:

- Configure the range of multicast groups that the current interface will work for in interface view.
- Configure the range of multicast groups that the interface corresponding to the VLAN where the current port resides will work for in Ethernet port view.

**Configuring a multicast group filter in VLAN interface view**

**Table 302** Configure a multicast group filter in VLAN interface view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configuring a multicast group filter:</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>In VLAN interface view</td>
<td>gmp group-policy acl-number [ 1</td>
<td>2</td>
</tr>
<tr>
<td>In LoopBack interface view</td>
<td>igmp group-policy acl-number [ 1</td>
<td>2 ]</td>
</tr>
</tbody>
</table>

**Configuring a multicast group filter in Ethernet port view**

**Table 303** Configure a multicast group filter in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configuring a multicast group filter</td>
<td>igmp group-policy acl-number vlan vlan-id</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No multicast group filter is configured by default. The port must belong to the specified VLAN.</td>
</tr>
</tbody>
</table>

**Configuring Simulated Joining**

Generally, hosts running IGMP respond to the IGMP query messages of the IGMP querier. If hosts fail to respond for some reason, the multicast router may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this from happening, you can configure a port of the IGMP-enabled VLAN interface as a multicast group member. When the port receives IGMP query messages, the simulated member host will respond. As a result, the subnet attached to the Layer 3 interface can continue to receive multicast traffic.
Through this configuration, the following functions can be implemented:

- When an Ethernet port is configured as a simulated member host, the switch sends an IGMP report through this port. Meanwhile, the simulated host sends the same IGMP report to itself and establishes a corresponding IGMP entry based on this report.

- When receiving an IGMP general query, the simulated host responds with an IGMP report. Meanwhile, the simulated host sends the same IGMP report to itself to ensure that the IGMP entry does not age out.

- When the simulated joining function is disabled on an Ethernet port, the simulated host sends an IGMP leave message.

Therefore, to ensure that IGMP entries will not age out, the port must receive IGMP general queries periodically.

### Configuring simulated joining in VLAN interface view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface Vlan-interface interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure one or more ports in the VLAN as simulated member host(s) of the specified multicast group:</td>
<td></td>
<td>Required Disabled by default</td>
</tr>
<tr>
<td>VLAN interface view</td>
<td><code>gmp host-join group-address port interface-list</code></td>
<td></td>
</tr>
<tr>
<td>LoopBack interface view</td>
<td><code>gmp host-join group-address</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring simulated joining in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the port in the specified VLAN as a simulated member host of the specified multicast group</td>
<td><code>igmp host-join group-address vlan vlan-id</code></td>
<td>Required Disabled by default</td>
</tr>
</tbody>
</table>

**CAUTION:**

- Before configuring simulated joining, you must enable IGMP in VLAN interface view first.

- If you configure simulated joining in Ethernet port view, the Ethernet port must belong to the specified VLAN; otherwise the configuration does not take effect.

- Generally, an interface serving as an IGMP querier cannot act as an IGMP proxy interface. If it is necessary to configure an IGMP querier interface as an IGMP proxy interface, you must configure the port that belongs to the proxy
interface and connects to the upstream multicast device as a static router port. For details, see Configuring a Static Router Port.

### Configuring IGMP Proxy

**Table 306  Configure IGMP Proxy**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface</td>
<td>-</td>
</tr>
<tr>
<td>Configure IGMP Proxy</td>
<td>igmp proxy Vlan-interface interface-number</td>
<td>Required, Disabled by default</td>
</tr>
</tbody>
</table>

**CAUTION:**

- You must enable the PIM protocol on the interface before configuring the `igmp proxy` command. Otherwise, the IGMP Proxy feature does not take effect.
- One interface cannot serve as the proxy interface for two or more interfaces.

### Removing Joined IGMP Groups from an Interface

You can remove all the joined multicast groups from a particular interface or all interfaces of the switch, or remove a particular multicast group address or group address range from a particular interface or all interfaces.

**Table 307  Remove joined multicast groups from one or all interfaces**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove the specified group or all groups from the specified interface or all interfaces</td>
<td>reset igmp group { all</td>
<td>interface interface-type interface-number { all</td>
</tr>
</tbody>
</table>

**CAUTION:** After a multicast group is removed from an interface, the multicast group can join the group again.

### Displaying IGMP

After completing the above-mentioned configurations, you can execute the `display` command in any view to verify the configuration by checking the displayed information.

**Table 308  Display IGMP**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the membership information of the IGMP multicast group</td>
<td>display igmp group [ group-address</td>
<td>interface interface-type interface-number ]</td>
</tr>
<tr>
<td>Display the IGMP configuration and running information of the interface</td>
<td>display igmp interface [ interface-type interface-number ]</td>
<td></td>
</tr>
</tbody>
</table>


PIM Overview

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging static routes or unicast routing tables generated by any unicast routing protocol, such as Routing Information Protocol (RIP), open shortest path first (OSPF), Intermediate System to Intermediate System (IS-IS), or Border Gateway Protocol (BGP). Independent of the unicast routing protocols running on the device, multicast routing can be implemented as long as the corresponding multicast routing entries are created through unicast routes. PIM uses the Reverse Path Forwarding (RPF) mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it is subject to an RPF check. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet; if the RPF check fails, the device discards the packet.

Based on the forwarding mechanism, PIM falls into two modes:

- Protocol Independent Multicast-Dense Mode (PIM-DM), and
- Protocol Independent Multicast-Sparse Mode (PIM-SM).

To facilitate description, a network comprising PIM-capable routers is referred to as a **PIM domain** in this document.

Introduction to PIM-DM

PIM-DM is a type of dense mode multicast protocol. It uses the **push mode** for multicast forwarding, and is suitable for small-sized networks with densely distributed multicast members.

The basic implementation of PIM-DM is as follows:

- PIM-DM assumes that at least one multicast group member exists on each subnet of a network, and therefore multicast data is flooded to all nodes on the network. Then, branches without multicast forwarding are pruned from the forwarding tree, leaving only those branches that contain receivers. This **flood and prune** process takes place periodically, that is, pruned branches resume multicast forwarding when the pruned state times out and then data is re-flooded down these branches, and then are pruned again.
- When a new receiver on a previously pruned branch joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch.

Generally speaking, the multicast forwarding path is a source tree, namely a forwarding tree with the multicast source as its **root** and multicast group members as its **leaves**. Because the source tree is the shortest path from the multicast source to the receivers, it is also called shortest path tree (SPT).
How PIM-DM Works

The working mechanism of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT building
- Graft
- Assert

Neighbor discovery

In a PIM domain, a PIM router discovers PIM neighbors, maintains PIM neighboring relationships with other routers, and builds and maintains SPTs by periodically multicasting hello messages to all other PIM routers (224.0.0.13).

*Every activated interface on a router sends hello messages periodically, and thus learns the PIM neighboring information pertinent to the interface.*

SPT building

The process of building an SPT is the process of **flood and prune**.

1. In a PIM-DM domain, when a multicast source $S$ sends multicast data to a multicast group $G$, the multicast packet is first flooded throughout the domain:
   - The router first performs RPF check on the multicast packet. If the packet passes the RPF check, the router creates an $(S, G)$ entry and forwards the data to all downstream nodes in the network. In the flooding process, an $(S, G)$ entry is created on all the routers in the PIM-DM domain.

2. Then, nodes without receivers downstream are pruned:
   - A router having no receivers downstream sends a prune message to the upstream node to **tell** the upstream node to delete the corresponding interface from the outgoing interface list in the $(S, G)$ entry and stop forwarding subsequent packets addressed to that multicast group down to this node.

   *An $(S, G)$ entry contains the multicast source address $S$, multicast group address $G$, outgoing interface list, and incoming interface.*

   *For a given multicast stream, the interface that receives the multicast stream is referred to as **upstream**, and the interfaces that forward the multicast stream are referred to as **downstream**.*

A prune process is first initiated by a leaf router. As shown in Figure 119, a router without any receiver attached to it (the router connected with Host A, for example) sends a prune message, and this prune process goes on until only necessary branches are left in the PIM-DM domain. These branches constitute the SPT.
The **flood and prune** process takes place periodically. A pruned state timeout mechanism is provided. A pruned branch restarts multicast forwarding when the pruned state times out and then is pruned again when it no longer has any multicast receiver.

> Pruning has a similar implementation in PIM-SM.

**Graft**

When a host attached to a pruned node joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch. The process is as follows:

1. The node that need to receive multicast data sends a graft message hop by hop toward the source, as a request to join the SPT again.
2. Upon receiving this graft message, the upstream node puts the interface on which the graft was received into the forwarding state and responds with a graft-ack message to the graft sender.
3. If the node that sent a graft message does not receive a graft-ack message from its upstream node, it will keep sending graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

**Assert**

If multiple multicast routers exist on a multi-access subnet, duplicate packets may flow to the same subnet. To shutoff duplicate flows, the assert mechanism is used for election of a single multicast forwarder on a multi-access network.
As shown in Figure 120, after Router A and Router B receive an \((S, G)\) packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own local interface, receive a duplicate packet forwarded by the other. Upon detecting this condition, both routers send an assert message to all PIM routers (224.0.0.13) through the interface on which the packet was received. The assert message contains the following information: the multicast source address \((S)\), the multicast group address \((G)\), and the preference and metric of the unicast route to the source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent \((S, G)\) packets on the multi-access subnet. The comparison process is as follows:

1. The router with a higher unicast route preference to the source wins;
2. If both routers have the same unicast route preference to the source, the router with a smaller metric to the source wins;
3. If there is a tie in route metric to the source, the router with a higher IP address of the local interface wins.

**Introduction to PIM-SM**

PIM-DM uses the *flood and prune* principle to build SPTs for multicast data distribution. Although an SPT has the shortest path, it is built with a low efficiency. Therefore the PIM-DM mod is not suitable for large- and medium-sized networks.

PIM-SM is a type of sparse mode multicast protocol. It uses the *pull mode* for multicast forwarding, and is suitable for large- and medium-sized networks with sparsely and widely distributed multicast group members.

The basic implementation of PIM-SM is as follows:

- PIM-SM assumes that no hosts need to receive multicast data. In the PIM-SM mode, routers must specifically request a particular multicast stream before the data is forwarded to them. The core task for PIM-SM to implement multicast forwarding is to build and maintain rendezvous point trees (RPTs). An RPT is rooted at a router in the PIM domain as the common node, or rendezvous point (RP), through which the multicast data travels along the RPT and reaches the receivers.
■ When a receiver is interested in the multicast data addressed to a specific multicast group, the router connected to this receiver sends a join message to the RP corresponding to that multicast group. The path along which the message goes hop by hop to the RP forms a branch of the RPT.

■ When a multicast source sends a multicast packet to a multicast group, the router directly connected with the multicast source first registers the multicast source with the RP by sending a register message to the RP by unicast. The arrival of this message at the RP triggers the establishment of an SPT. Then, the multicast source sends subsequent multicast packets along the SPT to the RP. Upon reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.

Multicast traffic is duplicated only where the distribution tree branches, and this process automatically repeats until the multicast traffic reaches the receivers.

How PIM-SM Works

The working mechanism of PIM-SM is summarized as follows:

■ Neighbor discovery
■ DR election
■ RP discovery
■ RPT building
■ Multicast source registration
■ Switchover from RPT to SPT
■ Assert

Neighbor discovery

PIM-SM uses exactly the same neighbor discovery mechanism as PIM-DM does. Refer to “Neighbor discovery” on page 414.

DR election

PIM-SM also uses hello messages to elect a designated router (DR) for a multi-access network. The elected DR will be the only multicast forwarder on this multi-access network.

A DR must be elected in a multi-access network, no matter this network connects to multicast sources or to receivers. The DR at the receiver side sends join messages to the RP; the DR at the multicast source side sends register messages to the RP.

■ A DR is elected on a multi-access subnet by means of comparison of the priorities and IP addresses carried in hello messages. An elected DR is substantially meaningful to PIM-SM. PIM-DM itself does not require a DR. However, if IGMPv1 runs on any multi-access network in a PIM-DM domain, a DR must be elected to act as the IGMPv1 querier on that multi-access network.

■ IGMP must be enabled on a device that acts as a DR before receivers attached to this device can join multicast groups through this DR.
As shown in Figure 121, the DR election process is as follows:

1. Routers on the multi-access network send hello messages to one another. The hello messages contain the router priority for DR election. The router with the highest DR priority will become the DR.

2. In the case of a tie in the router priority, or if any router in the network does not support carrying the DR-election priority in hello messages, the router with the highest IP address will win the DR election.

When the DR fails, a timeout in receiving hello message triggers a new DR election process among the other routers.

- The Switch 5500 does not support DR priority. DR election is based on IP addresses.
- In a PIM-DM domain, a DR serves as an IGMPv1 querier.

**RP discovery**

The RP is the core of a PIM-SM domain. For a small-sized, simple network, one RP is enough for forwarding information throughout the network, and the position of the RP can be statically specified on each router in the PIM-SM domain. In most cases, however, a PIM-SM network covers a wide area and a huge amount of multicast traffic needs to be forwarded through the RP. To lessen the RP burden and optimize the topological structure of the RPT, each multicast group should have its own RP. Therefore, a bootstrap mechanism is needed for dynamic RP election. For this purpose, a bootstrap router (BSR) should be configured.

As the administrative core of a PIM-SM domain, the BSR collects advertisement messages (C-RP-Adv messages) from candidate-RPs (C-RPs) and chooses the appropriate C-RP information for each multicast group to form an RP-Set, which is a database of mappings between multicast groups and RPs. The BSR then floods the RP-Set to the entire PIM-SM domain. Based on the information in these RP-Sets, all routers (including the DRs) in the network can calculate the location of the corresponding RPs.
A PIM-SM domain (or an administratively scoped region) can have only one BSR, but can have multiple candidate-BSRs (C-BSRs). Once the BSR fails, a new BSR is automatically elected from the C-BSRs through the bootstrap mechanism to avoid service interruption. Similarly, multiple C-RPs can be configured in a PIM-SM domain, and the position of the RP corresponding to each multicast group is calculated through the BSR mechanism.

Figure 122 shows the positions of C-RPs and the BSR in the network.

**Figure 122**  BSR and C-RPs

**RPT building**

**Figure 123**  Building an RPT in PIM-SM
As shown in Figure 123, the process of building an RPT is as follows:

1. When a receiver joins a multicast group G, it uses an IGMP message to inform the directly connected DR.

2. Upon getting the receiver information, the DR sends a join message, which is hop by hop forwarded to the RP corresponding to the multicast group.

3. The routers along the path from the DR to the RP form an RPT branch. Each router on this branch generates a (*, G) entry in its forwarding table. The * means any multicast source. The RP is the root, while the DRs are the leaves, of the RPT.

The multicast data addressed to the multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer interested in the multicast data addressed to a multicast group G, the directly connected DR sends a prune message, which goes hop by hop along the RPT to the RP. Upon receiving the prune message, the upstream node deletes its link with this downstream node from the outgoing interface list and checks whether it itself has receivers for that multicast group. If not, the router continues to forward the prune message to its upstream router.

**Multicast source registration**

The purpose of multicast source registration is to inform the RP about the existence of the multicast source.

**Figure 124**  Multicast registration

As shown in Figure 124, the multicast source registers with the RP as follows:

1. When the multicast source S sends the first multicast packet to a multicast group G, the DR directly connected with the multicast source, upon receiving the
multicast packet, encapsulates the packet in a PIM register message, and sends the message to the corresponding RP by unicast.

2 When the RP receives the register message, on one hand, it extracts the multicast packet from the register message and forwards the multicast packet down the RPT, and, on the other hand, it sends an (S, G) join message hop by hop toward the multicast source. Thus, the routers along the path from the RP to the multicast source constitute an SPT branch. Each router on this branch generates a (S, G) entry in its forwarding table. The multicast source is the root, while the RP is the leaf, of the SPT.

3 The subsequent multicast data from the multicast source travels along the established SPT to the RP, and then the RP forwards the data along the RPT to the receivers. When the multicast traffic arrives at the RP along the SPT, the RP sends a register-stop message to the source-side DR by unicast to stop the source registration process.

**Switchover from RPT to SPT**

Initially, multicast traffic flows along an RPT from the RP to the receivers. Because the RPT is not necessarily the tree that has the shortest path, upon receiving the first multicast packet along the RPT, the receiver-side DR initiates an RPT-to-SPT switchover process, as follows:

1 First, the receiver-side DR sends an (S, G) join message hop by hop to the multicast source. When the join message reaches the source-side DR, all the routers on the path have installed the (S, G) entry in their forwarding table, and thus an SPT branch is established.

2 Subsequently, the receiver-side DR sends a prune message hop by hop to the RP. Upon receiving this prune message, the RP forwards it towards the multicast source, thus to implement RPT-to-SPT switchover.

After the RPT-to-SPT switchover, multicast data can be directly sent from the source to the receivers. PIM-SM builds SPTs through RPT-to-SPT switchover more economically than PIM-DM does through the *flood and prune* mechanism.

**Assert**

PIM-SM uses exactly the same assert mechanism as PIM-DM does. Refer to “Configuring PIM-DM” on page 421.

### Configuring PIM-DM

#### Enabling PIM-DM

With PIM-DM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from PIM neighbors. When deploying a PIM-DM domain, you are recommended to enable PIM-DM on all interfaces of non-border routers.

<table>
<thead>
<tr>
<th>Table 309 Configure a PIM filter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
</tbody>
</table>
| Enable multicast routing | `multicast routing-enable` | Required  
Disabled by default |
Configuring PIM-SM

Table 309  Configure a PIM filter

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter interface view</td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Enable PIM-DM</td>
<td>pim dm</td>
<td>Required, Disabled by default</td>
</tr>
</tbody>
</table>

Table 310  Configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling PIM-SM”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring an RP”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring a BSR”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Filtering the Registration Packets from DR to RP”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Disabling RPT-to-SPT Switchover”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Enabling PIM-SM

With PIM-SM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from PIM neighbors. When deploying a PIM-SM domain, you are recommended to enable PIM-SM on all interfaces of non-border routers (border routers are PIM-enabled routers located on the boundary of BSR admin-scope regions).

Table 311  Enable PIM-SM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable multicast routing</td>
<td>multicast routing-enable</td>
<td>Required, Disabled by default</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Enable PIM-SM</td>
<td>pim sm</td>
<td>Required, Disabled by default</td>
</tr>
</tbody>
</table>

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just a backup means for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

Configuring a static RP

If there is only one dynamic RP in a network, manually configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR. To enable a static RP to work normally, you must perform this configuration on all the routers in the PIM-SM domain and specify the same RP address.
Follow the steps in Table 312 to configure a static RP:

Table 312  Configuring a static RP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>-</td>
</tr>
<tr>
<td>Configure a static RP</td>
<td>static-rp rp-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>acl-number</td>
<td>No static RP by default</td>
</tr>
</tbody>
</table>

Configuring a C-RP

In a PIM-SM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. We recommend that you configure C-RPs on backbone routers.

To guard against C-RP spoofing, you need to configure a legal C-RP address range and the range of multicast groups to be served on the BSR. In addition, because every C-BSR has a chance to become the BSR, you need to configure the same filtering policy on all C-BSRs in the PIM-SM domain.

Follow the steps in Table 313 to configure a C-RP:

Table 313  Configuring a C-RP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>-</td>
</tr>
<tr>
<td>Configure candidate RPs</td>
<td>c-rp interface-type</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>By default, candidate RPs are not set for the switch and the value of priority is 0.</td>
</tr>
<tr>
<td></td>
<td>group-policy acl-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>priority priority</td>
<td></td>
</tr>
<tr>
<td>Limit the range of valid</td>
<td>crp-policy acl-number</td>
<td>Optional</td>
</tr>
<tr>
<td>C-RPs</td>
<td></td>
<td>By default, the range of valid C-RPs is not set for the switch.</td>
</tr>
</tbody>
</table>

- If the range of multicast groups that an RP serves is not specified when the RP is configured, the RP serves all multicast groups.
- If the configured static RP address is the address of an UP interface on the local switch, the switch will serve as an RP.
- Static RPs do not take effect when the RP generated by the BSR mechanism takes effect.

Configuring a BSR

A PIM-SM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the PIM-SM domain.
Configuring a C-BSR

C-BSRs should be configured on routers in the backbone network. When configuring a router as a C-BSR, be sure to specify a PIM-SM-enabled interface on the router. The BSR election process is summarized as follows:

- Initially, every C-BSR assumes itself to be the BSR of this PIM-SM domain, and uses its interface IP address as the BSR address to send bootstrap messages.
- When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in message. The C-BSR with a higher priority wins. If there is a tie in the priority, the C-BSR with a higher IP address wins. The loser uses the winner’s BSR address to replace its own BSR address and no longer assumes itself to be the BSR, while the winner retains its own BSR address and continues assuming itself to be the BSR.

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thus to prevent a maliciously configured host from masquerading as a BSR. The same configuration needs to be made on all routers in the PIM-SM domain. The following are typical BSR spoofing cases and the corresponding preventive measures:

- Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and discard unwanted messages.
- When a router in the network is controlled by an attacker or when an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win BSR election to control the right of advertising RP information in the network. After being configured as a C-BSR, a router automatically floods the network with bootstrap messages. As a bootstrap message has a TTL value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

The above-mentioned preventive measures can partially protect the security of BSRs in a network. However, if a legal BSR is controlled by an attacker, the above-mentioned problem will still occur.

Follow the the steps in Table 314 to configure a C-BSR

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>-</td>
</tr>
<tr>
<td>Configure an interface as</td>
<td>c-bsr</td>
<td>Optional</td>
</tr>
<tr>
<td>a C-BSR</td>
<td>interface-type</td>
<td>No C-BSRs are configured by default.</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>The default priority is 0.</td>
</tr>
<tr>
<td></td>
<td>hash-mask-len [ priority ]</td>
<td></td>
</tr>
</tbody>
</table>
Only one C-BSR is in effect on a Layer 3 switch at a time.

**Configuring a PIM-SM domain border**

As the administrative core of a PIM-SM domain, the BSR sends the collected RP-Set information in the form of bootstrap messages to all routers in the PIM-SM domain.

A PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of PIM domain border interfaces partition a network into different PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that can become a PIM-SM domain border.

Follow the steps in Table 315 to configure a PIM-SM domain border:

**Table 314 Configuring a C-BSR**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a legal BSR address</td>
<td><code>bsr-policy acl-number</code></td>
<td>Optional No restrictions on BSR address range by default</td>
</tr>
</tbody>
</table>

**Caution:** After this feature is configured, Bootstrap messages cannot pass the border. However, the other PIM messages can pass the domain border. The network can be effectively divided into domains that use different BSRs.

**Filtering the Registration Packets from DR to RP**

Within a PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different multicast source or group addresses. You can configure a filtering rule to filter register messages so that the RP can serve specific multicast groups. If an (S, G) entry is denied by the filtering rule, or the action for this entry is not defined in the filtering rule, the RP will send a register-stop message to the DR to stop the registration process for the multicast data.

Follow the steps in Table 316 to filter the registration packets from RP to DR.

**Table 315 Configuring a PIM-SM domain border**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure a PIM-SM domain border</td>
<td><code>pim bsr-boundary</code></td>
<td>Optional By default, no PIM-SM domain border is configured.</td>
</tr>
</tbody>
</table>

**Table 316 Filtering the registration packets from RP to DR**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td><code>pim</code></td>
<td>-</td>
</tr>
</tbody>
</table>
CHAPTER 37: PIM CONFIGURATION

Table 316  Filtering the registration packets from RP to DR

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure to filter the registration packets</td>
<td>register-policy acl-number</td>
<td>Optional by default, the switch does not filter the registration packets from DR.</td>
</tr>
<tr>
<td>from RP to DR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Caution: Only the registration packets matching the permit command of ACLs can be accepted. When an invalid ACL is defined, RP will reject all the registration packets.

Disabling RPT-to-SPT Switchover

Initially, a PIM-SM-enabled multicast device forwards multicast packets through an RPT. By default, the last-hop switch initiates an RPT-to-SPT switchover process. You can also disable RPT-to-SPT switchover through the configuration.

Table 317  Disable RPT-to-SPT switchover

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>-</td>
</tr>
<tr>
<td>Disable RPT-to-SPT switchover</td>
<td>spt-switch-threshold infinity [ group-policy acl-number [ order order-value ] ]</td>
<td>Optional by default, the device switches to the SPT immediately after it receives the first multicast packet from the RPT.</td>
</tr>
</tbody>
</table>

Typically, you need to configure the above-mentioned parameters on the receiver-side DR and the RP only. Since both the DR and RP are elected, however, you should carry out these configurations on the routers that may win DR election and on the C-RPs that may win RP election.

Displaying PIM

After completing the above-mentioned configurations, you can execute the following display commands in any view to verify the configuration by checking the displayed information.
Table 318 Display PIM

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display PIM multicast routing tables</td>
<td>display pim routing-table { { *g [ group-address { mask { mask-length</td>
<td>mask } }</td>
</tr>
<tr>
<td>Display the information about PIM interfaces</td>
<td>display pim interface { interface-type interface-number }</td>
<td></td>
</tr>
<tr>
<td>Display the information about PIM neighbor routers</td>
<td>display pim neighbor [ interface interface-type interface-number ]</td>
<td></td>
</tr>
<tr>
<td>Display BSR information</td>
<td>display pim bsr-info</td>
<td></td>
</tr>
<tr>
<td>Display RP information</td>
<td>display pim rp-info [ group-address ]</td>
<td></td>
</tr>
</tbody>
</table>

Table 319 PIM Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Multicast Data Filter</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Hello Interval</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring PIM Neighbors</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring Multicast Source Lifetime</td>
<td>Optional</td>
</tr>
<tr>
<td>Clearing the Related PIM Entries</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configuring a Multicast Data Filter

No matter in a PIM-DM domain or a PIM-SM domain, routers can check passing-by multicast data based on the configured filtering rules and determine whether to continue forwarding the multicast data. In other words, PIM routers can act as multicast data filters. These filters can help implement traffic control on one hand, and control the information available to receivers downstream to enhance data security on the other hand.

Follow the steps in Table 320 to configure a multicast data filter:

Table 320 Configuring a multicast data filter

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>—</td>
</tr>
<tr>
<td>Configure a multicast group filter</td>
<td>source-policy acl-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No multicast data filter by default</td>
</tr>
</tbody>
</table>

Caution:
- If you have configured a basic ACL, the switch filters all the received multicast packets based on the multicast source address, and discards packets that fail source address match.
If you have configured an advanced ACL, the switch filters all the received multicast packets based on the multicast source address and group address, and discards packets that fail source and group address match.

Configuring the Hello Interval

In a PIM domain, a PIM router discovers PIM neighbors and maintains PIM neighboring relationships with other routers by periodically sending hello messages.

Follow the steps in Table 321 to configure the Hello interval:

Table 321 Configuring the Hello Interval

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure the Hello interval on the interface</td>
<td>pim timer hello seconds</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default Hello interval is 30 seconds.</td>
</tr>
</tbody>
</table>

Caution: Before configuring related PIM functions, you must enable PIM-DM or PIM-SM first.

Configuring PIM Neighbors

In order to prevent plenty of PIM neighbors from exhausting the memory of the router, which may result in router failure, you can limit the number of PIM neighbors on the router interface. However, the total number of PIM neighbors of a router is defined by the system, and you cannot modify it through commands.

You can define what Layer 3 switches can become PIM neighbors of the current interface by configuring a basic ACL.

Follow the steps in Table 322 to configure PIM neighbors:

Table 322 Configuring PIM Neighbors

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Configure a limit on the number of PIM neighbors on the interface</td>
<td>pim neighbor-limit limit</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the upper limit on the number of PIM neighbors on an interface is 128.</td>
</tr>
<tr>
<td>Configure a filtering rule to filter PIM neighbors</td>
<td>pim neighbor-policy acl-number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no filtering rule is configured.</td>
</tr>
</tbody>
</table>

Caution: If the number of existing PIM neighbors exceeds the user-defined limit, the existing PIM neighbors will not be deleted.

Configuring Multicast Source Lifetime

Initially, some data is lost when multicast receivers receive multicast data from a multicast source. The reason is that (S, G) entries in the PIM routing table and
multicast routing table age out if no data stream is received within a configurable period of time (the aging time of these entries is also called multicast source lifetime). These entries need to be reestablished before the corresponding multicast data can be forwarded by the multicast switch again. In the process of table entry reestablishment, some data may be lost.

If the multicast source lifetime is appropriately lengthened when the data traffic has stopped, the multicast data, when arriving at the multicast switch again, can be forwarded by the switch without the need of reestablishing the table entries. This avoid data loss.

Follow the steps in Table 323 to configure multicast source lifetime:

Table 323 Configuring Multicast Source Lifetime

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter PIM view</td>
<td>pim</td>
<td>—</td>
</tr>
<tr>
<td>Configure multicast source</td>
<td>source-lifetime interval</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>210 seconds by default</td>
</tr>
</tbody>
</table>

Caution: The aging time configuration acts on all \((S, G)\) entries in the PIM routing table and the multicast routing table, but not on specific \((S, G)\) entry. The configuration changes the aging time of all the existing \((S, G)\) entries.

Clearing the Related PIM Entries

You can execute the reset command in user view to clear the related statistics about multicast PIM.

Follow the steps in Table 324 to clear the related PIM entries:

Table 324 Clearing the Related PIM Entries

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear PIM route entries</td>
<td>reset pim routing-table { all \</td>
<td>{ group-address [ mask group-mask ]</td>
</tr>
<tr>
<td>Clear PIM neighbors</td>
<td>reset pim neighbor { all \</td>
<td>{ neighbor-address</td>
</tr>
</tbody>
</table>
Displaying and Maintaining PIM

Follow the steps in Table 325 to display and maintain PIM.

**Table 325** Displaying and Maintaining PIM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display PIM multicast routing tables</td>
<td><code>display pim routing-table</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the information about PIM interfaces</td>
<td><code>display pim interface</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the information about PIM neighbor routers</td>
<td><code>display pim neighbor</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display BSR information</td>
<td><code>display pim bsr-info</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display RP information</td>
<td><code>display pim rp-info</code></td>
<td>Available in any view</td>
</tr>
</tbody>
</table>

**PIM Configuration Examples**

**PIM-DM Configuration Example**

**Network requirements**

- Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain operates in the dense mode.
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D through VLAN-interface 103.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch D through VLAN-interface 101 and VLAN-interface 102 respectively.
- IGMP is required on Switch A, Switch B, Switch C, and hosts in N1 and N2. Switch B is the IGMP querier on the multi-access subnet.
Network diagram

Figure 125  Network diagram for PIM-DM configuration

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan-int100</td>
<td>10.110.1.1/24</td>
<td>Switch D</td>
<td>Vlan-int300</td>
<td>10.110.5.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan-int103</td>
<td>192.168.1.1/24</td>
<td></td>
<td>Vlan-int103</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td></td>
<td>192.168.1.1/24</td>
<td>4</td>
<td></td>
<td>192.168.1.2/24</td>
<td>4</td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int200</td>
<td>10.110.2.1/24</td>
<td>Switch D</td>
<td>Vlan-int101</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan-int101</td>
<td>192.168.2.1/24</td>
<td></td>
<td>Vlan-int102</td>
<td>192.168.3.1/24</td>
</tr>
<tr>
<td></td>
<td>192.168.2.1/24</td>
<td>4</td>
<td></td>
<td>192.168.3.1/24</td>
<td>4</td>
</tr>
<tr>
<td>Switch C</td>
<td>Vlan-int200</td>
<td>10.110.2.2/24</td>
<td></td>
<td>Vlan-int102</td>
<td>192.168.3.2/24</td>
</tr>
<tr>
<td></td>
<td>Vlan-int102</td>
<td>192.168.3.2/24</td>
<td></td>
<td>192.168.3.2/24</td>
<td>4</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure the interface IP addresses and unicast routing protocol for each switch

Configure the IP address and subnet mask for each interface as per Figure 125. Detailed configuration steps are omitted here.

Configure the OSPF protocol for interoperation among the switches in the PIM-DM domain. Ensure the network-layer interoperation among Switch A, Switch B, Switch C and Switch D in the PIM-DM domain and enable dynamic update of routing information among the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

2. Enable IP multicast routing, and enable PIM-DM on each interface
# Enable IP multicast routing on Switch A, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 100, which connects Switch A to the stub network.

```plaintext
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

The configuration on Switch B and Switch C is similar to the configuration on Switch A.

# Enable IP multicast routing on Switch D, and enable PIM-DM on each interface.

```plaintext
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

**Verifying the configuration**

Use the `display pim neighbor` command to view the PIM neighboring relationships among the switches. For example:

```plaintext
# View the PIM neighboring relationships on Switch D.

[SwitchD] display pim neighbor
Neighbor's Address Interface Name Uptime Expires
192.168.1.1 Vlan-interface1 00:47:08 00:01:39
192.168.2.1 Vlan-interface1 00:48:05 00:01:29
192.168.3.1  Vlan-interface1 00:49:08 00:01:34
```

Use the `display pim routing-table` command to view the PIM routing table information on each switch. For example:

```plaintext
# View the PIM routing table information on Switch A.

<SwitchA> display pim routing-table
PIM-DM Routing Table
Total 1 (S,G) entry

(10.110.5.100, 225.1.1.1)
```
Protocol 0x40: PIMDM, Flag 0xC: SPT NEG_CACHE
Uptime: 00:00:23, Timeout in 187 sec
Upstream interface: Vlan-interface103, RPF neighbor: 192.168.1.2
Downstream interface list:
  Vlan-interface100, Protocol 0x1: IGMP, never timeout

Matched 1 (S,G) entry

The information on Switch B and Switch C is similar to that on Switch A.

# View the PIM routing table information on Switch D.

<SwitchD> display pim routing-table
PIM-DM Routing Table
Total 1 (S,G) entry

(10.110.5.100, 225.1.1.1)
  Protocol 0x40: PIMDM, Flag 0xC: SPT NEG_CACHE
  Uptime: 00:00:23, Timeout in 187 sec
  Upstream interface: Vlan-interface300, RPF neighbor: NULL
  Downstream interface list:
    Vlan-interface101, Protocol 0x200: SPT, timeout in 147 sec
    Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec
    Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec

Matched 1 (S,G) entry

PIM-SM Configuration Example

Network requirements

- Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain operates in the sparse mode (not divided into different BSR admin-scope regions).
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- Switch E connects to Switch A, Switch B, Switch C and Switch D, and its VLAN-interface 102 interface acts a C-BSR and a C-RP, with the range of multicast groups served by the C-RP being 225.1.1.0/24.
Network diagram

**Figure 126** Network diagram for PIM-SM domain configuration

### Configuration procedure

1. Configure the interface IP addresses and unicast routing protocol for each switch.

   Configure the IP address and subnet mask for each interface as per Figure 126. Detailed configuration steps are omitted here.

   Configure the OSPF protocol for interoperation among the switches in the PIM-SM domain. Ensure the network-layer interoperation among Switch A, Switch B, Switch C, Switch D and Switch E in the PIM-SM domain and enable dynamic update of routing information among the switches through a unicast routing protocol. Detailed configuration steps are omitted here.
2 Enable IP multicast routing, and enable PIM-SM on each interface

# Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and enable IGMP on VLAN-interface 100, which connects Switch A to the stub network.

<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable IGMP on the corresponding interfaces on these two switches.

3 Configure a C-BSR and a C-RP

# Configure the service scope of RP advertisements and the positions of the C-BSR and C-RP on Switch E.

<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
[SwitchE-pim] quit

Verifying the configuration

# Display PIM neighboring relationships on Switch E.

<SwitchE> display pim neighbor
Neighbor’s Address Interface Name Uptime Expires
192.168.9.1 Vlan-interface102 02:47:04 00:01:42
192.168.2.1 Vlan-interface103 02:45:04 00:04:46
192.168.3.1 Vlan-interface104 02:42:24 00:04:45
192.168.4.2 Vlan-interface105 02:43:44 00:05:44

# Display BSR information on Switch E.

<SwitchE> display pim bsr-info
Current BSR Address: 192.168.9.2
Priority: 0
Mask Length: 24
Expires: 00:01:39
Local host is BSR
# Display RP information on Switch E.

```bash
<SwitchE> display pim rp-info
PIM-SM RP-SET information:
BSR is: 192.168.9.2

Group/MaskLen: 225.1.1.0/24
  RP 192.168.9.2
  Version: 2
  Priority: 0
  Uptime: 00:49:44
  Expires: 00:01:46
```

# Display PIM routing table information on Switch A.

```bash
<SwitchA> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry

(*, 225.1.1.1), RP 192.168.9.2
  Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
  Uptime: 00:23:21, never timeout
  Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout
(10.110.5.100, 225.1.1.1)
  Protocol 0x20: PIMSM, Flag 0x80004: SPT
  Uptime: 00:03:43, Timeout in 199 sec
  Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout
Matched 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry
```

The displayed information of Switch B and Switch C is similar to that of Switch A.

# Display PIM routing table information on Switch D.

```bash
<SwitchD> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

(10.110.5.100, 225.1.1.1)
  Protocol 0x20: PIMSM, Flag 0x4: SPT
  Uptime: 00:03:03, Timeout in 27 sec
  Upstream interface: Vlan-interface300, RPF neighbor: NULL
  Downstream interface list:
    Vlan-interface101, Protocol 0x200: SPT, timeout in 147 sec
    Vlan-interface105, Protocol 0x200: SPT, timeout in 145 sec
Matched 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry
```

# Display PIM routing table information on Switch E.

```bash
<SwitchE> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry

(*, 225.1.1.1), RP 192.168.9.2
```
Troubleshooting PIM

**Symptom:** The router cannot set up multicast routing tables correctly.

**Solution:** You can troubleshoot PIM according to the following procedure.

- Make sure that the unicast routing is correct before troubleshooting PIM.
- Because PIM-SM needs the support of RP and BSR, you must execute the `display pim bsr-info` command to see whether BSR information exists. If not, you must check whether there is any unicast route to the BSR. Then, use the `display pim rp-info` command to check whether the RP information is correct. If RP information does not exist, you must check whether there is any unicast route to RP.
- Use the `display pim neighbor` command to check whether the neighboring relationship is correctly established.
Because multicast source discovery protocol (MSDP) does not support the IRF feature, MSDP cannot be configured in Fabric.

MSTP Overview

Introduction to MSDP
Multicast source discovery protocol (MSDP) is an inter-domain multicast solution developed to address the interconnection of protocol independent multicast sparse mode (PIM-SM) domains. It is used to discover multicast source information in other PIM-SM domains.

In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information of a domain is isolated from that of another domain. As a result, the RP is aware of the source information only within the local domain and a multicast distribution tree is built only within the local domain to deliver multicast data from a local multicast source to local receivers. If there is a mechanism that allows RPs of different PIM-SM domains to share their multicast source information, the local RP will be able to join multicast sources in other domains and multicast data can be transmitted among different domains.

MSDP achieves this objective. By establishing MSDP peer relationships among RPs of different PIM-SM domains, source active (SA) messages can be forwarded among domains and the multicast source information can be shared.

CAUTION:
- MSDP is applicable only if the intra-domain multicast protocol is PIM-SM.
- MSDP is meaningful only for the any-source multicast (ASM) model.

How MSDP Works
MSDP peers
With one or more pairs of MSDP peers configured in the network, an MSDP interconnection map is formed, where the RPs of different PIM-SM domains are interconnected in series. Relayed by these MSDP peers, an SA message sent by an RP can be delivered to all other RPs.
As shown in Figure 127, an MSDP peer can be created on any PIM-SM router. MSDP peers created on PIM-SM routers that assume different roles function differently.

1 MSDP peers on RPs

- Source-side MSDP peer: the MSDP peer nearest to the multicast source (Source), typically the source-side RP, like RP 1. The source-side RP creates SA messages and sends the messages to its remote MSDP peer to notify the MSDP peer of the locally registered multicast source information. A source-side MSDP must be created on the source-side RP; otherwise it will not be able to advertise the multicast source information out of the PIM-SM domain.

- Receiver-side MSDP peer: the MSDP peer nearest to the receivers, typically the source-side RP, like RP 3. Upon receiving an SA message, the receiver-side MSDP peer resolves the multicast source information carried in the message and joins the SPT rooted at the source across the PIM-SM domain. When multicast data from the multicast source arrives, the receiver-side MSDP peer forwards the data to the receivers along the RPT.

- Intermediate MSDP peer: an MSDP peer with multicast remote MSDP peers, like RP 2. An intermediate MSDP peer forwards SA messages received from one remote MSDP peer to other remote MSDP peers, functioning as a relay of multicast source information.

2 MSDP peers created on common PIM-SM routers (other than RPs)

Router A and Router B are MSDP peers on common multicast routers. Such MSDP peers just forward received SA messages.

An RP is dynamically elected from C-RPs. To enhance network robustness, a PIM-SM network typically has more than one C-RP. As the RP election result is unpredictable, MSDP peering relationships should be built among all C-RPs so that the winner C-RP is always on the MSDP interconnection map, while the losing C-RPs will assume the role of common PIM-SM routers on the MSDP interconnection map.
Implementing inter-domain multicast delivery by leveraging MSDP peers

As shown in Figure 128, an active source (Source) exists in the domain PIM-SM 1, and RP 1 has learned the existence of Source through multicast source registration. If RPs in PIM-SM 2 and PIM-SM 3 also wish to know the specific location of Source so that receiver hosts can receive multicast traffic originated from it, MSDP peering relationships should be established between RP 1 and RP 3 and between RP 3 and RP 2 respectively.

**Figure 128  MSDP peering relationships**

The process for implementing inter-domain multicast delivery by leveraging MSDP peers is as follows:

1. When the multicast source in PIM-SM 1 sends the first multicast packet to multicast group G, DR 1 encapsulates the multicast data within a register message and sends the register message to RP 1. Then, RP 1 gets aware of the information related to the multicast source.

2. As the source-side RP, RP 1 creates SA messages and periodically sends the SA messages to its MSDP peer. An SA message contains the source address (S), the multicast group address (G), and the address of the RP which has created this SA message (namely RP 1).

3. On MSDP peers, each SA message is subject to a reverse path forwarding (RPF) check and multicast policy-based filtering, so that only SA messages that have arrived along the correct path and passed the filtering are received and forwarded. This avoids delivery loops of SA messages. In addition, you can configure MSDP peers into an MSDP mesh group so as to avoid flooding of SA messages between MSDP peers.

4. SA messages are forwarded from one MSDP peer to another, and finally the information of the multicast source traverses all PIM-SM domains with MSDP peers (PIM-SM 2 and PIM-SM 3 in this example).
Upon receiving the SA message create by RP 1, RP 2 in PIM-SM 2 checks whether there are any receivers for the multicast group in the domain.

- If so, the RPT for the multicast group G is maintained between RP 2 and the receivers. RP 2 creates an (S, G) entry, and sends an (S, G) join message hop by hop towards DR 1 at the multicast source side, so that it can directly join the SPT rooted at the source over other PIM-SM domains. Then, the multicast data can flow along the SPT to RP 2 and is forwarded by RP 2 to the receivers along the RPT. Upon receiving the multicast traffic, the DR at the receiver side (DR 2) decides whether to initiate an RPT-to-SPT switchover process.

- If no receivers for the group exist in the domain, RP 2 does not create an (S, G) entry and does join the SPT rooted at the source.

An MSDP mesh group refers to a group of MSDP peers that have MSDP peering relationships among one another and share the same group name.

When using MSDP for inter-domain multicasting, once an RP receives information from a multicast source, it no longer relies on RPs in other PIM-SM domains. The receivers can override the RPs in other domains and directly join the multicast source based SPT.

**RPF check rules for SA messages**

As shown in Figure 129, there are five autonomous systems in the network, AS 1 through AS 5, with IGP enabled on routers within each AS and EBGP as the interoperation protocol among different ASs. Each AS contains at least one PIM-SM domain and each PIM-SM domain contains one or more RPs. MSDP peering relationships have been established among different RPs. RP 3, RP 4 and RP 5 are in an MSDP mesh group. On RP 7, RP 6 is configured as its static RPF peer.

*If only one MSDP peer exists in a PIM-SM domain, this PIM-SM domain is also called a stub domain. For example, AS 4 in Figure 129 is a stub domain. The MSDP peer in a stub domain can have multiple remote MSDP peers at the same time. You can configure one or more remote MSDP peers as static RPF peers. When an RP receives an SA message from a static RPF peer, the RP accepts the SA message and forwards it to other peers without performing an RPF check.*

*Figure 129* Diagram for RPF check for SA messages
As illustrated in Figure 129, these MSDP peers dispose of SA messages according to the following RPF check rules:

1. When RP 2 receives an SA message from RP 1

   Because the source-side RP address carried in the SA message is the same as the MSDP peer address, which means that the MSDP peer where the SA is from is the RP that has created the SA message, RP 2 accepts the SA message and forwards it to its other MSDP peer (RP 3).

2. When RP 3 receives the SA message from RP 2

   Because the SA message is from an MSDP peer (RP 2) in the same AS, and the MSDP peer is the next hop on the optimal path to the source-side RP, RP 3 accepts the message and forwards it to other peers (RP 4 and RP 5).

3. When RP 4 and RP 5 receive the SA message from RP 3

   Because the SA message is from an MSDP peer (RP 3) in the same mesh group, RP 4 and RP 5 both accept the SA message, but they do not forward the message to other members in the mesh group; instead, they forward it to other MSDP peers (RP 6 in this example) out of the mesh group.

4. When RP 6 receives the SA messages from RP 4 and RP 5 (suppose RP 5 has a higher IP address)

   Although RP 4 and RP 5 are in the same SA (AS 3) and both are MSDP peers of RP 6, because RP 5 has a higher IP address, RP 6 accepts only the SA message from RP 5.

5. When RP 7 receives the SA message from RP 6

   Because the SA message is from a static RPF peer (RP 6), RP 7 accepts the SA message and forwards it to other peer (RP 8).

6. When RP 8 receives the SA message from RP 7

   An EBGP route exists between two MSDP peers in different ASs. Because the SA message is from an MSDP peer (RP 7) in a different AS, and the MSDP peer is the next hop on the EBGP route to the source-side RP, RP 8 accepts the message and forwards it to its other peer (RP 9).

7. When RP 9 receives the SA message from RP 8

   Because RP 9 has only one MSDP peer, RP 9 accepts the SA message.

   SA messages from other paths than described above will not be accepted nor forwarded by MSDP peers.

Implementing intra-domain Anycast RP by leveraging MSDP peers

Anycast RP refers to such an application that enables load balancing and redundancy backup between two or more RPs within a PIM-SM domain by configuring the same IP address for, and establishing MSDP peering relationships between, these RPs.
As shown in Figure 130, within a PIM-SM domain, a multicast source sends multicast data to multicast group G, and Receiver is a member of the multicast group. To implement Anycast RP, configure the same IP address (known as anycast RP address, typically a private address) on Router A and Router B, configure these interfaces as C-RPs, and establish an MSDP peering relationship between Router A and Router B.

*Usually an Anycast RP address is configured on a logic interface, like a loopback interface.*

**Figure 130** Typical network diagram of Anycast RP

![Diagram of Anycast RP](image)

The work process of Anycast RP is as follows:

1. The multicast source registers with the nearest RP. In this example, Source registers with RP 1, with its multicast data encapsulated in the register message. When the register message arrives to RP 1, RP 1 decapsulates the message.

2. Receivers send join messages to the nearest RP to join in the RPT rooted as this RP. In this example, Receiver joins the RPT rooted at RP 2.

3. RPs share the registered multicast information by means of SA messages. In this example, RP 1 creates an SA message and sends it to RP 2, with the multicast data from Source encapsulated in the SA message. When the SA message reaches RP 2, RP 2 decapsulates the message.

4. Receivers receive the multicast data along the RPT and directly joins the SPT rooted at the multicast source. In this example, RP 2 forwards the multicast data down the RPT. When Receiver receives the multicast data from Source, it directly joins the SPT rooted at Source.

The significance of Anycast RP is as follows:

- **Optimal RP path:** A multicast source registers with the nearest RP so that an SPT with the optimal path is built; a receiver joins the nearest RP so that an RPT with the optimal path is built.

- **Load balancing between RPs:** Each RP just needs to maintain part of the source/group information within the PIM-SM domain and forward part of the multicast data, thus achieving load balancing between different RPs.
Redundancy backup between RPs: When an RP fails, the multicast source previously registered on it or the receivers previously joined it will register with or join another nearest RP, thus achieving redundancy backup between RPs.

**CAUTION:**
- Be sure to configure a 32-bit subnet mask (255.255.255.255) for the Anycast RP address, namely configure the Anycast RP address into a host address.
- An MSDP peer address must be different from the Anycast RP address.

**Protocols and Standards**
MSDP is documented in the following specifications:
- RFC 3618: Multicast Source Discovery Protocol (MSDP)
- RFC 3446: Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

**Configuring MSDP Basic Functions**
A route is required between two routers that are MSDP peers to each other. Through this route, the two routers can transfer SA messages between PIM-SM domains. For an area containing only one MSDP peer, known as a stub area, the route is not compulsory. SA messages are transferred in a stub area through the configuration of static RPF peers. In addition, the use of static RPF peers can avoid RPF check on the received SA messages, thus saving resources.

Before configuring static RPF peers, you must create an MSDP peering connection. If you configure only one MSDP peer on a router, the MSDP peer will act as a static RPF peer. If you configure multiple RPF peers, you need to handle them by using different rules according to the configured policies.

When configuring multiple static RPF peers for the same router, you must follow the following two configuration methods:

- In the case that all the peers use the `rp-policy` keyword: Multiple static RPF peers function at the same time. RPs in SA messages are filtered based on the configured prefix list, and only the SA messages whose RP addresses pass the filtering are received. If multiple static RPF peers using the same `rp-policy` keyword are configured, when any of the peers receives an SA message, it will forward the SA message to other peers.

- None of the peers use the `rp-policy` keyword: Based on the configured sequence, only the first static RPF peer whose connection state is UP is active. All the SA messages from this peer will be received, while the SA messages from other static RPF peers will be discarded. Once the active static RPF peer fails (because the configuration is removed or the connection is terminated), based on the configuration sequence, the subsequent first static RPF peer whose connection is in the UP state will be selected as the active static RPF peer.

**Configuration Prerequisites**
Before configuring basic MSDP functions, you need to configure:
- A unicast routing protocol
- PIM-SM basic functions
Configuring MSDP Basic Functions

An AS may contain multiple MSDP peers. To avoid SA flooding between the MSDP peers, you can use the MSDP mesh mechanism to improve traffic. When multiple MSDP peers are fully connected with one another, these MSDP peers form a mesh group. When an MSDP peer in the mesh group receives SA messages from outside the mesh group, it sends them to other members of the group. On the other hand, a mesh group member does not perform RPF check on SA messages from within the mesh group and does not forward the messages to other members of the mesh group. This avoids SA message flooding since it is unnecessary to run BGP or MBGP between MSDP peers, thus simplifying the RPF checking mechanism.

The sessions between MSDP peers can be terminated and reactivated sessions as required. When a session between MSDP peers is terminated, the TCP connection is closed, and there will be no reconnection attempts. However, the configuration information is kept.

Configuration Prerequisites

Before configuring an MSDP peer connection, you need to configure:

- A unicast routing protocol
- Basic functions of IP multicast
- PIM-SM basic functions
- MSDP basic functions

Table 326 Configure MSDP basic functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable MSDP function and enter MSDP view</td>
<td>msdp</td>
<td>Required</td>
</tr>
<tr>
<td>Create an MSDP peer connection</td>
<td>peer peer-address connect-interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a static RPF peer</td>
<td>static-rpf-peer peer-address [ rp-policy ip-prefix-name ]</td>
<td>Optional</td>
</tr>
</tbody>
</table>

No MSDP peer connection is created by default.

No static RFP is configured by default.

Configuring Description Information for MSDP Peers

You can configure description information for each MSDP peer to manage and memorize the MSDP peers.
Configuring Connection Between MSDP Peers

Configuring an MSDP Mesh Group

Configure a mesh group name on all the peers that will become members of the MSDP mesh group so that the peers are fully connected with one another in the mesh group.

Before you configure an MSDP mesh group, make sure that the routers are fully connected with one another.

The same group name must be configured on all the peers before they can join a mesh group.

If you add the same MSDP peer to multiple mesh groups, only the latest configuration takes effect.

Configuring MSDP Peer Connection Control

The connection between MSDP peers can be flexibly controlled. You can disable the MSDP peering relationships temporarily by shutting down the MSDP peers. As a result, SA messages cannot be transmitted between these two peers. On the other hand, when resetting an MSDP peering relationship between faulty MSDP peers or bringing faulty MSDP peers back to work, you can adjust the retry interval of establishing a peering relationship through the following configuration.

### Table 328  Configure description information for an MSDP peer

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
<td>-</td>
</tr>
<tr>
<td>Configure description information for an MSDP peer</td>
<td>peer peer-address description text</td>
<td>Optional By default, an MSDP peer has no description information.</td>
</tr>
</tbody>
</table>

### Table 329  Configure an MSDP mesh group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
<td>-</td>
</tr>
<tr>
<td>Add an MSDP peer to a mesh group</td>
<td>peer peer-address mesh-group name</td>
<td>Required By default, an MSDP peer does not belong to any mesh group.</td>
</tr>
</tbody>
</table>

### Table 330  Configure MSDP peer connection control

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
<td>-</td>
</tr>
<tr>
<td>Shut down the connection with the specified MSDP peer</td>
<td>shutdown peer-address</td>
<td>Optional By default, all MSDP peering connections are up.</td>
</tr>
<tr>
<td>Configure the retry interval of MSDP peer connection establishment</td>
<td>timer retry seconds</td>
<td>Optional 30 seconds by default</td>
</tr>
</tbody>
</table>
Configuring SA Message Transmission

An SA message contains the IP address of the multicast source $S$, multicast group address $G$, and RP address. In addition, it contains the first multicast data received by the RP in the domain where the multicast source resides. For some burst multicast data, if the multicast data interval exceeds the SA message hold time, the multicast data must be encapsulated in the SA message; otherwise, the receiver will never receive the multicast source information.

By default, when a new receiver joins, a router does not send any SA request message to its MSDP peer but has to wait for the next SA message. This defers the reception of the multicast information by the receiver. In order for the new receiver to know about the currently active multicast source as quickly as possible, the router needs to send SA request messages to the MSDP peer.

Generally, a router accepts all SA messages sent by all MSDP peers and sends all SA messages to all MSDP peers. By configuring the rules for filtering SA messages to receive/send, you can effectively control the transmission of SA messages among MSDP peers. For forwarded SA messages, you can also configure a Time-to-Live (TTL) threshold to control the range where SA messages carrying encapsulated data are transmitted.

To reduce the delay in obtaining the multicast source information, you can cache SA messages on the router. The number of SA messages cached must not exceed the system limit. The more messages are cached, the more router memory is occupied.

Configuration Prerequisites

Before you configure SA message transmission, perform the following tasks:

- Configuring a unicast routing protocol.
- Configuring basic IP multicast functions.
- Configuring basic PIM-SM functions.
- Configuring basic MSDP functions.

### Table 331 Configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring RP Address in SA Messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring SA Message Cache”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Transmission and Filtering of SA Request Messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring a Rule for Filtering the Multicast Sources of SA Messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring a Rule for Filtering Received and Forwarded SA Messages”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configuring RP Address in SA Messages

IMSDP peers deliver SA messages to one another. Upon receiving an SA message, a router performs an RPF check on the message. If the router finds that the remote RP address is the same as the local RP address, it will discard the SA message. In anycast RP application, however, you need to configure RPs with the same IP address on two or more routers in the same PIM-SM domain, and configure these RPs as MSDP peers to one another. Therefore, a logic RP address (namely the RP address on a logic interface) that is different from the actual RP address must be designated for SA messages so that the messages can pass the RPF check.
In Anycast RP application, a C-BSR and a C-RP must be configured on different devices or ports.

Configuring SA Message Cache

With the SA message caching mechanism enabled on the router, the group that a new member subsequently joins can obtain all active sources directly from the SA cache and join the corresponding SPT source tree, instead of waiting for the next SA message.

You can configure the number of SA entries cached in each MSDP peer on the router by executing the following command, but the number must be within the system limit. To protect a router against Denial of Service (DoS) attacks, you can manually configure the maximum number of SA messages cached on the router. Generally, the configured number of SA messages cached should be less than the system limit.

<table>
<thead>
<tr>
<th>Table 332</th>
<th>Configure RP address in SA messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
</tr>
<tr>
<td>Configure the address of the specified interface as the RP address in SA messages</td>
<td>originating-rp interface-type interface-number</td>
</tr>
</tbody>
</table>

In Anycast RP application, a C-BSR and a C-RP must be configured on different devices or ports.

Configuring the Transmission and Filtering of SA Request Messages

After you enable the sending of SA request messages, when a router receives a Join message, it sends an SA request message to the specified remote MSDP peer, which responds with an SA message that it has cached. After sending an SA request message, the router will get immediately a response from all active multicast sources. The SA message that the remote MSDP peer responds with is cached in advance; therefore, you must enable the SA message caching mechanism in advance. Typically, only the routers caching SA messages can respond to SA request messages.

After you have configured a rule for filtering received SA messages, if no ACL is specified, all SA request messages sent by the corresponding MSDP peer will be ignored; if an ACL is specified, the SA request messages that satisfy the ACL rule are received while others are ignored.

<table>
<thead>
<tr>
<th>Table 333</th>
<th>Configure SA message cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
</tr>
<tr>
<td>Enable SA message caching mechanism</td>
<td>cache-sa-enable</td>
</tr>
<tr>
<td>Configure the maximum number of SA messages that can be cached</td>
<td>peer peer-address sa-cache-maximum sa-limit</td>
</tr>
</tbody>
</table>
CHAPTER 38: MSDP CONFIGURATION

Configuring a Rule for Filtering the Multicast Sources of SA Messages

An RP filters each registered source to control the information of active sources advertised in the SA message. An MSDP peer can be configured to advertise only the (S, G) entries in the multicast routing table that satisfy the filtering rule when the MSDP creates the SA message; that is, to control the (S, G) entries to be imported from the multicast routing table to the PIM-SM domain. If the import-source command is executed without the acl keyword, no source will be advertised in the SA message.

<table>
<thead>
<tr>
<th>Table 334</th>
<th>Configure the transmission and filtering of SA request messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
</tr>
<tr>
<td>Enable SA message caching mechanism</td>
<td>cache-sa-enable</td>
</tr>
<tr>
<td>Enable MSDP peers to send SA request messages</td>
<td>peer peer-address request-sa-enable</td>
</tr>
<tr>
<td>Configure a rule for filtering the SA messages received by an MSDP peer</td>
<td>peer peer-address sa-request-policy</td>
</tr>
</tbody>
</table>

| acl-number |

Configuring a Rule for Filtering Received and Forwarded SA Messages

Besides the creation of source information, controlling multicast source information allows you to control the forwarding and reception of source information. You can control the reception of SA messages using the MSDP inbound filter (corresponding to the import keyword); you can control the forwarding of SA messages by using either the MSDP outbound filter (corresponding to the export argument) or the TTL threshold. By default, an MSDP peer receives and forwards all SA messages.

MSDP inbound/outbound filter implements the following functions:

- Filtering out all (S, G) entries
- Receiving/forwarding only the SA messages permitted by advanced ACL rules (You can configure ACL rules for filtering source IP addresses and group IP addresses.)

<table>
<thead>
<tr>
<th>Table 335</th>
<th>Configure a rule for filtering multicast sources using SA messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td>msdp</td>
</tr>
<tr>
<td>Configure to filter multicast sources using SA messages</td>
<td>import-source [ acl acl-number ]</td>
</tr>
</tbody>
</table>

| acl-number |
An SA message carrying encapsulated data can reach the specified MSDP peer outside the domain only if the TTL in its IP header is greater than the threshold; therefore, you can control the forwarding range of SA messages that carry encapsulated data by configuring the TTL threshold.

**Table 336  Configure a rule for filtering received and forwarded SA messages**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter MSDP view</td>
<td><code>msdp</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure to filter imported and exported SA messages</td>
<td>`peer peer-address sa-policy { import</td>
<td>export } [ acl acl-number ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no filtering is imposed on SA messages to be received or forwarded, namely all SA messages from MSDP peers are received or forwarded.</td>
</tr>
<tr>
<td>Configure the minimum TTL required for a multicast packet to be sent to the specified MSDP peer</td>
<td><code>peer peer-address minimum-ttl ttl-value</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the value of TTL threshold is 0.</td>
</tr>
</tbody>
</table>

**Displaying and Maintaining MSDP Configuration**

After the above-mentioned configuration, you can use the following `display` commands in any view to display the MSDP running information, so as to verify configuration result.

In user view, you can execute the following `reset` commands to reset MSDP statistics.

**Table 337  Display and maintain MSDP configuration**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the brief information of MSDP peer state</td>
<td><code>display msdp brief</code></td>
<td>You can execute the <code>display</code> commands in any view.</td>
</tr>
<tr>
<td>Display the detailed information of MSDP peer status</td>
<td><code>display msdp peer-status [ peer-address ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the (S, G) state learned from MSDP peers</td>
<td>`display msdp sa-cache [ group-address</td>
<td>source-address</td>
</tr>
<tr>
<td>Display the number of sources and groups in the MSDP cache</td>
<td><code>display msdp sa-count [ autonomous-system-number ]</code></td>
<td></td>
</tr>
<tr>
<td>Reset the TCP connection with the specified MSDP peer</td>
<td><code>reset msdp peer peer-address</code></td>
<td>You can execute the <code>reset</code> commands in user view.</td>
</tr>
<tr>
<td>Clear the cached SA messages</td>
<td><code>reset msdp sa-cache [ group-address ]</code></td>
<td></td>
</tr>
<tr>
<td>Clear the statistics information of the specified MSDP peer without resetting the MSDP peer</td>
<td><code>reset msdp statistics [ peer-address ]</code></td>
<td></td>
</tr>
</tbody>
</table>
Tracing the transmission path of an SA message over the network

You can use the `msdp-tracert` command in any view to trace the path along which the multicast data travels from the multicast source to the destination receiver over the network, so as to locate errors, if any.

**Table 338** Trace the transmission path of an SA message over the network

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace the transmission path of an SA message over the network</td>
<td>`msdp-tracert source-address group-address rp-address [max-hops max-hops] [next-hop-info</td>
<td>sa-info</td>
</tr>
<tr>
<td>Trace the transmission path of messages sent by the multicast source over the network</td>
<td>`mtracert source-address [group-address</td>
<td>last-hop-router-address group-address]</td>
</tr>
</tbody>
</table>

You can locate message loss and configuration errors by tracing the network path of the specified (S, G, RP) entries. Once the transmission path of SA messages is determined, correct configuration can prevent the flooding of SA messages.

**MSDP Configuration Example**

**Example of Anycast RP Application**

**Network requirements**

- The PIM-SM domain has multiple multicast sources and receivers. OSPF runs within the domain to provide unicast routes.
- You must configure the anycast RP feature so that the receiver-side DRs and the source-side DRs can initiate a Join message to their respective RPs that are in the topologically nearest to them.
- On Switch B and Switch D, configure the interface Loopback 10 as a C-BSR, and Loopback 20 as a C-RP.
- The router ID of Switch B is 1.1.1.1, while the router ID of Switch D is 2.2.2.2. Set up an MSDP peering relationship between Switch B and Switch D.
Network diagram

Figure 131  Network diagram for anycast RP configuration (on switches)

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source 1</td>
<td>-</td>
<td>10.110.5.100/24</td>
<td>Switch C</td>
<td>Vlan-int101</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Source 2</td>
<td>-</td>
<td>10.110.6.100/24</td>
<td>Switch C</td>
<td>Vlan-int102</td>
<td>192.168.2.2/24</td>
</tr>
<tr>
<td>Switch A</td>
<td>Vlan-int300</td>
<td>10.110.5.1/24</td>
<td>Switch D</td>
<td>Vlan-int200</td>
<td>10.110.3.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan-int103</td>
<td>10.110.2.2/24</td>
<td></td>
<td>Vlan-int104</td>
<td>10.110.4.1/24</td>
</tr>
<tr>
<td>Switch B</td>
<td>Vlan-int100</td>
<td>10.110.1.1/24</td>
<td></td>
<td>Vlan-int102</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan-int103</td>
<td>10.110.2.1/24</td>
<td>Loop0</td>
<td>2.2.2.2/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vlan-int101</td>
<td>192.168.1.1/24</td>
<td>Loop10</td>
<td>4.4.4.4/32</td>
<td></td>
</tr>
<tr>
<td>Loop0</td>
<td>1.1.1.1/32</td>
<td></td>
<td>Loop20</td>
<td>10.1.1.1/32</td>
<td></td>
</tr>
<tr>
<td>Loop10</td>
<td>3.3.3.3/32</td>
<td></td>
<td>Switch E</td>
<td>Vlan-int400</td>
<td>10.110.6.1/24</td>
</tr>
<tr>
<td>Loop20</td>
<td>10.1.1.1/32</td>
<td></td>
<td></td>
<td>Vlan-int104</td>
<td>10.110.4.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1  Configure the interface IP addresses and unicast routing protocol for each switch

Configure the IP address and subnet mask for each interface as per Figure 131. Detailed configuration steps are omitted here.

Configure OSPF for interconnection between the switches. Ensure the network-layer interoperability among the switches, and ensure the dynamic update of routing information between the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

2  Enable IP multicast routing, and enable PIM-SM and IGMP.
# Enable IP multicast routing on Switch B, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 100.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim sm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
[SwitchB] interface Vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] interface loopback 10
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
[SwitchB] interface loopback 20
[SwitchB-LoopBack20] pim sm
[SwitchB-LoopBack20] quit
```

The configuration on Switch A, Switch C, Switch D, and Switch E is similar to the configuration on Switch B.

3 Configure C-BSRs and C-RPs.

```
# Configure Loopback 10 as a C-BSR and configure Loopback 20 as a C-RP on Switch B.

[SwitchB] pim
[SwitchB-pim] c-bsr loopback 10 24
[SwitchB-pim] c-rp loopback 20
[SwitchB-pim] quit
```

The configuration on Switch D is similar to the configuration on Switch B.

4 Configure MSDP peers

```
# Configure an MSDP peer on Loopback 0 of Switch B.

[SwitchB] msdp
[SwitchB-msdp] originating-rp loopback 0
[SwitchB-msdp] peer 2.2.2.2 connect-interface loopback 0
[SwitchB-msdp] quit
```

# Configure an MSDP peer on Loopback 0 of Switch D.

```
[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback 0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback 0
[SwitchD-msdp] quit
```

5 Verify the configuration
You can use the display msdp brief command to view the brief information of MSDP peering relationships between the switches.

# View the brief MSDP peer information on Switch B.

[SwitchB] display msdp brief
MSDP Peer Brief Information
Peer's Address     State Up/Down time    AS     SA Count   Reset Count
2.2.2.2            Up        00:48:21        ?      2          0

# View the brief MSDP peer information on Switch D.

[SwitchD] display msdp brief
MSDP Peer Brief Information
Peer's Address     State Up/Down time    AS     SA Count   Reset Count
1.1.1.1            Up        00:50:22        ?      2          0

When Source 1 (10.110.5.100/24) sends multicast data to multicast group G (225.1.1.1), Receiver 1 joins multicast group G. By comparing the PIM routing information displayed on Switch B with that displayed on Switch D, you can see that Switch B now acts as the RP for Source 1 and Receiver 1. Source 1 registers with Switch B and Receiver 1 sends a join message to Switch B.

# View the PIM routing information on Switch B.

[Switch B] display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry
(*, 225.1.1.1), RP 10.1.1.1
  Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
  Uptime: 00:00:13, never timeout
  Upstream interface: Null, RPF neighbor: 0.0.0.0
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout
(10.110.5.100, 225.1.1.1)
  Protocol 0x20: PIMSM, Flag 0x4: SPT
  Uptime: 00:03:08, Timeout in 206 sec
  Upstream interface: Vlan-interface103, RPF neighbor: NULL
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout
Matched 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry

# View the PIM routing information on Switch D.

[SwitchD] display pim routing-table
PIM-SM Routing Table
Total 0 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry
Matched 0 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

---

**Troubleshooting MSDP Configuration**

**MSDP Peer Always in the Down State**

**Symptom**

An MSDP peer is configured, but it is always in the down state.
Analysis
An MSDP peer relationship between the locally configured connect-interface interface address and the configured peer address is based on a TCP connection. If the address of local connect-interface interface is inconsistent with the peer address configured on the peer router, no TCP connection can be established. If there is no route between the two peers, no TCP connection can be established.

Solution
1 Check the connectivity of the route between the routers. Use the display ip routing-table command to check that the unicast route between the routers is correct.
2 Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3 Check that the interface addresses of the MSDP peers are consistent. Use the display current-configuration command to check that the address of the local connect-interface interface is consistent with the address of the corresponding MSDP peer.

No SA Entry in the SA Cache of the Router
Symptom
An MSDP fails to send \((S, G)\) forwarding entries through an SA message.

Analysis
You can use the import-source command to send the \((S, G)\) entries of the local multicast domain to the neighboring MSDP peer through SA messages. The acl keyword is optional. If you do not use this keyword, all \((S, G)\) entries will be filtered out by default, that is, none of the \((S, G)\) entries in the local multicast domain will be advertised. Before the import-source command is executed, the system will send all \((S, G)\) entries in the local multicast domain. If the MSDP fails to send the \((S, G)\) entries of the local multicast domain through SA messages, verify that the import-source command is configured correctly.

Solution
1 Check the connectivity of the route between the routers. Use the display ip routing-table command to check that the unicast route between the routers is correct.
2 Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3 Verify the configuration of the import-source command and the corresponding ACL to ensure that the ACL rule filters the right \((S, G)\) entries.
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 132, 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. However, multicast packets for unknown multicast groups are still broadcast at Layer 2.

Figure 132  Before and after IGMP Snooping is enabled on Layer 2 device

Basic Concepts in IGMP Snooping

IGMP Snooping related ports

As shown in Figure 133, 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).
Port aging timers in IGMP Snooping and related messages and actions

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Message before expiry</th>
<th>Action after expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router port aging timer</td>
<td>For each router port, the switch sets a timer initialized to the aging time of the route port</td>
<td>IGMP general query or PIM hello</td>
<td>The switch removes this port from its router port list</td>
</tr>
<tr>
<td>Member port aging timer</td>
<td>When a port joins a multicast group, the switch sets a timer for the port, which is initialized to the member port aging time</td>
<td>IGMP membership report</td>
<td>The switch removes this port from the multicast group forwarding table</td>
</tr>
</tbody>
</table>

Work Mechanism of IGMP Snooping

A switch running IGMP Snooping performs different actions when it receives different IGMP messages, as follows:
When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers 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 router port existing in its router port list, the switch resets the aging timer of this router port.
- If the receiving port is not a router port existing in its router port list, the switch adds it into its router port list and sets an aging timer for this router port.

When receiving a membership report

A host sends an IGMP report to the multicast router 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 multicast router 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 multicast group the host is interested in, and performs the following to the receiving port:

- If the port is already in the forwarding table, the switch resets the member port aging timer of the port.
- If the port is not in the forwarding table, the switch installs an entry for this port in the forwarding table and starts the member port aging timer of this port.

A switch will not forward an IGMP report through a non-router port for the following reason: Due to the IGMP report suppression mechanism, if member hosts of that multicast group still exist under non-router ports, the hosts will stop sending reports when they receive the message, and this prevents the switch from knowing if members of that multicast group are still attached to these ports.

For the description of IGMP report suppression mechanism, refer to “Work Mechanism of IGMPv1” on page 403.

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 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 to announce that it has left the multicast group.

Upon receiving an IGMP leave message on the last member port, a switch forwards it out all router ports in the VLAN. Because the switch does not know whether any other member hosts of that multicast group still exists under the port to which the IGMP leave message arrived, the switch does not immediately delete the forwarding entry corresponding to that port from the forwarding table; instead, it resets the aging timer of the member port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left 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, a switch forwards it through all the router ports in the VLAN and all member ports of that multicast group, and performs the following to the receiving port:

- If any IGMP report in response to the group-specific query arrives to the member port before its aging timer expires, this means that some other members of that multicast group still exist under that port: the switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query arrives to the member port before its aging timer expires as a response to the IGMP group-specific query, this means that no members of that multicast group still exist under the port: the switch deletes the forwarding entry corresponding to the port from the forwarding table when the aging timer expires.

⚠️ **CAUTION:** After an Ethernet switch enables IGMP Snooping, when it receives the IGMP leave message sent by a host in a multicast group, it judges whether the multicast group exists automatically. If the multicast group does not exist, the switch drops this IGMP leave message.

### Configuring IGMP Snooping

The following table lists all the IGMP Snooping configuration tasks:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Enabling IGMP Snooping&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring the Version of IGMP Snooping&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Timers&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Fast Leave Processing&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Multicast Group Filter&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the Maximum Number of Multicast Groups on a Port&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring IGMP Snooping Querier&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Suppressing Flooding of Unknown Multicast Traffic in a VLAN&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Static Member Port for a Multicast Group&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Static Router Port&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Port as a Simulated Group Member&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a VLAN Tag for Query Messages&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Enabling IGMP Snooping

Table 340 IGMP Snooping configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring Multicast VLAN”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Enabling IGMP Snooping

Table 341 Enable IGMP Snooping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP Snooping globally</td>
<td>igmp-snooping enable</td>
<td>Required (By default, IGMP Snooping is disabled globally.)</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP Snooping on the VLAN</td>
<td>igmp-snooping enable</td>
<td>Required (By default, IGMP Snooping is disabled on all the VLANs.)</td>
</tr>
</tbody>
</table>

CAUTION:
- Although both Layer 2 and Layer 3 multicast protocols can run on the same switch simultaneously, they cannot run simultaneously on a VLAN or its corresponding VLAN interface.
- Before enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping settings will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for queries. For details, see “Configuring a VLAN Tag for Query Messages”.

Configuring the Version of IGMP Snooping

With the development of multicast technologies, IGMPv3 has found increasingly wide application. In IGMPv3, a host can not only join a specific multicast group but also explicitly specify to receive or reject the information from a specific multicast source. Working with PIM-SSM, IGMPv3 enables hosts to join specific multicast sources and groups directly, greatly simplifying multicast routing protocols and optimizing the network topology.

Table 342 Configure the version of IGMP Snooping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure the version of IGMP Snooping</td>
<td>igmp-snooping version version-number</td>
<td>Optional (The default IGMP Snooping version is version 2.)</td>
</tr>
</tbody>
</table>

CAUTION:
- Before configuring related IGMP Snooping functions, you must enable IGMP Snooping in the specified VLAN.
Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.

Configuring Timers

This section describes how to configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

Table 343  Configure timers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the aging timer of the router port</td>
<td>igmp-snooping router-aging-time seconds</td>
<td>Optional By default, the aging time of the router port is 105 seconds.</td>
</tr>
<tr>
<td>Configure the query response timer</td>
<td>igmp-snooping max-response-time seconds</td>
<td>Optional By default, the query response timeout time is 10 seconds.</td>
</tr>
<tr>
<td>Configure the aging timer of the multicast member port</td>
<td>igmp-snooping host-aging-time seconds</td>
<td>Optional By default, the aging time of multicast member ports is 260 seconds</td>
</tr>
</tbody>
</table>

Configuring Fast Leave Processing

With fast leave processing enabled, when the switch receives an IGMP leave message on a port, the switch directly removes that port from the forwarding table entry for the specific group. If only one host is attached to the port, enable fast leave processing to improve bandwidth management.

Enabling fast leave processing in system view

Table 344  Enable fast leave processing in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable fast leave processing</td>
<td>igmp-snooping fast-leave [ vlan vlan-list ]</td>
<td>Required By default, the fast leave processing feature is disabled.</td>
</tr>
</tbody>
</table>

Enabling fast leave processing in Ethernet port view

Table 345  Enable fast leave processing in Ethernet view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable fast leave processing for specific VLANs</td>
<td>igmp-snooping fast-leave [ vlan vlan-list ]</td>
<td>Required By default, the fast leave processing feature is disabled.</td>
</tr>
</tbody>
</table>

The fast leave processing function works for a port only if the host attached to the port runs IGMPv2 or IGMPv3.
The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).

The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

If fast leave processing and unknown multicast packet dropping or non-flooding are enabled on a port to which more than one host is connected, when one host leaves a multicast group, the other hosts connected to port and interested in the same multicast group will fail to receive multicast data for that group.

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 ACL rule configured on the receiving port. If the receiving port can join this multicast group, the switch adds this port to the IGMP Snooping multicast group list; 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.

Make sure that an ACL rule has been configured before configuring this feature.

Configuring a multicast group filter in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure a multicast group filter</td>
<td>igmp-snooping group-policy acl-number [ vlan vlan-list ]</td>
<td>Required No group filter is configured by default, namely hosts can join any multicast group.</td>
</tr>
</tbody>
</table>

Configuring a multicast group filter in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure a multicast group filter</td>
<td>igmp-snooping group-policy acl-number [ vlan vlan-list ]</td>
<td>Optional No group filter is configured by default, namely hosts can join any multicast group.</td>
</tr>
</tbody>
</table>

A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.

Table 346 Configure a multicast group filter in system view

Table 347 Configure a multicast group filter in Ethernet port view

- A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.
CHAPTER 39: IGMP SNOOPING CONFIGURATION

- If no ACL rule is configured, all the multicast groups will be filtered.
- Since most devices broadcast unknown multicast packets by default, this function is often used together with the function of dropping unknown multicast packets to prevent multicast streams from being broadcast as unknown multicast packets to a port blocked by this function.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring the Maximum Number of Multicast Groups 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.

<table>
<thead>
<tr>
<th>Table 348</th>
<th>Configure the maximum number of multicast groups on a port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Limit the number of multicast groups on a port</td>
<td>igmp-snooping group-limit limit [ vlan vlan-list [ overflow-replace ] ]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- To prevent bursting traffic in the network or performance deterioration of the device caused by excessive multicast groups, you can set the maximum number of multicast groups that the switch should process.
- When the number of multicast groups exceeds the configured limit, the switch removes its multicast forwarding entries starting from the oldest one. In this case, the multicast packets for the removed multicast group(s) will be flooded in the VLAN as unknown multicast packets. As a result, non-member ports can receive multicast packets within a period of time. To avoid this from happening, enable the function of dropping unknown multicast packets.

Configuring 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 querier 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 general queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.
You can also configure the source address, maximum response time and interval of general queries to be sent from the IGMP Snooping querier.

### Table 349 Configure IGMP Snooping querier

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td>igmp-snooping enable</td>
<td>Required By default, IGMP Snooping is disabled.</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td>igmp-snooping enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enable IGMP Snooping querier</td>
<td>igmp-snooping querier</td>
<td>Required By default, IGMP Snooping querier is disabled.</td>
</tr>
<tr>
<td>Configure the interval between IGMP general queries</td>
<td>igmp-snooping query-interval seconds</td>
<td>Optional By default, the interval between IGMP general queries is 60 seconds.</td>
</tr>
<tr>
<td>Configure the source IP address of IGMP general queries</td>
<td>igmp-snooping general-query source-ip current-interface</td>
<td>Optional By default, the source IP address of IGMP general queries is 0.0.0.0.</td>
</tr>
</tbody>
</table>

### Supressing Flooding of Unknown Multicast Traffic in a VLAN

With IGMP Snooping enabled in a VLAN, multicast traffic for unknown multicast groups is flooded within the VLAN by default. This wastes network bandwidth and affects multicast forwarding efficiency.

With the unknown multicast flooding suppression function enabled, when receiving a multicast packet for an unknown multicast group, an IGMP Snooping switch creates a nonflooding entry and relays the packet to router ports only, instead of flooding the packet within the VLAN. If the switch has no router ports, it drops the multicast packet.

### Table 350 Suppress flooding of unknown multicast traffic in the VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable unknown multicast flooding suppression</td>
<td>igmp-snooping nonflooding-enable</td>
<td>Required By default, unknown multicast flooding suppression</td>
</tr>
</tbody>
</table>

- If the function of dropping unknown multicast packets or the IRF fabric function is enabled, you cannot enable unknown multicast flooding suppression.
- Unknown multicast flooding suppression and multicast source port suppression cannot take effect at the same time. If both are enabled, only multicast source port suppression takes effect. In this case, multicast data received on the blocked port will be dropped.
CHAPTER 39: IGMP SNOOPING CONFIGURATION

Configuring Static Member Port for a Multicast Group

If the host connected to a port is interested in the multicast data for a specific group, you can configure that port as a static member port for that multicast group.

In Ethernet port view

Table 351  Configure a static multicast group member port in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the current port as</td>
<td><code>multicast static-group group-address vlan vlan-id</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no port is configured as a static multicast group member port.</td>
</tr>
</tbody>
</table>

In VLAN interface view

Table 352  Configure a static multicast group member port in VLAN interface view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface vlan-interface interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure specified port(s) as static member port(s) of a multicast group in the VLAN</td>
<td><code>multicast static-group group-address interface interface-list</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

CAUTION:

- You can configure up to 200 static member ports on the Switch 5500.
- If a port has been configured as an IRF fabric port or a reflect port, it cannot be configured as a static member port.

Configuring a Static Router Port

In a network where the topology is unlikely to change, you can configure a port on the switch as a static router port, so that the switch has a static connection to a multicast router and receives IGMP messages from that router.

In Ethernet port view

Table 353  Configure a static router port in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the current port as</td>
<td><code>multicast static-router-port vlan vlan-id</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no static router port is configured.</td>
</tr>
</tbody>
</table>
In VLAN view

Table 354  Configure a static router port in VLAN view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>—</td>
</tr>
<tr>
<td>Configure a specified port as a</td>
<td>multicast static-router-port</td>
<td>Required</td>
</tr>
<tr>
<td>a static router port</td>
<td>interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>By default, no static router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port is configured.</td>
</tr>
</tbody>
</table>

Simulated joining in IGMP Snooping is implemented in the same way as in IGMP except that IGMP Snooping establishes and maintains IGMP Snooping entries.

Enabling simulated joining in VLAN interface view

Follow the steps in Table 355 to enable simulated joining in VLAN interface view:

Table 355  Enabling simulated joining in VLAN interface view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Enable simulated joining</td>
<td>igmp host-join [ group-address ]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>source-ip source-address ] port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-list</td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>

Configuring simulated joining in in Ethernet port view

Follow the steps in Table 356 to configure a port as a simulated group member:

Table 356  Configure a port as a simulated group member

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the current port as a</td>
<td>igmp host-join [ group-address ]</td>
<td>Required</td>
</tr>
<tr>
<td>a simulated multicast group</td>
<td>source-ip source-address ] vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>member</td>
<td>interface-list</td>
<td>Simulated joining is disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by default.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- Before configuring a simulated host, enable IGMP Snooping in VLAN view first.
- The port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.
- You can use the source-ip source-address command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect when GMGPv3 Snooping is enabled in the VLAN.

Configuring a VLAN Tag for Query Messages

By configuring the VLAN tag carried in IGMP general and group-specific queries forwarded and sent by IGMP Snooping switches and by configuring the VLAN...
mapping function, you can enable multicast packet forwarding between different VLANs in a Layer-2 multicast network environment.

For description about VLAN mapping, see “QoS Profile Configuration” on page 709.

### Table 357 Configure VLAN Tag for query message

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td><strong>igmp-snooping enable</strong></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, IGMP Snooping is disabled.</td>
</tr>
<tr>
<td>Configure a VLAN tag for query messages</td>
<td><strong>igmp-snooping vlan-mapping vlan vlan-id</strong></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the VLAN tag in IGMP general and group-specific query messages is not changed.</td>
</tr>
</tbody>
</table>

You should not configure this function while the multicast VLAN function is in effect.

### Configuring Multicast VLAN

In traditional multicast implementations, when users in different VLANs listen to the same multicast group, the multicast data is copied on the multicast router for each VLAN that contains receivers. This is a big waste of network bandwidth.

In an IGMP Snooping environment, by configuring a multicast VLAN and adding ports to the multicast VLAN, you can allow users in different VLANs to share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN. In addition, because the multicast VLAN is isolated from user VLANs, this method also enhances the information security.

Multicast VLAN is mainly used in Layer 2 switching, but you must make the corresponding configurations on the Layer 3 switch.

### Table 358 Configure multicast VLAN on the Layer 3 switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Create a multicast VLAN and enter VLAN view</td>
<td><strong>vlan vlan-id</strong></td>
<td>-</td>
</tr>
<tr>
<td>Return to system view</td>
<td><strong>quit</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><strong>interface Vlan-interface vlan-id</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP</td>
<td><strong>igmp enable</strong></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IGMP feature is disabled.</td>
</tr>
<tr>
<td>Return to system view</td>
<td><strong>quit</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view for the Layer 2 switch to be configured</td>
<td><strong>interface interface-type interface-number</strong></td>
<td>-</td>
</tr>
</tbody>
</table>
One port can belong to only one multicast VLAN.

The port connected to a user terminal must be a hybrid port.

The multicast member ports must be in the same VLAN with the router port. Otherwise, the multicast member port cannot receive multicast packets.

If a router port is in a multicast VLAN, the router port must be configured as a trunk port or a hybrid port that allows tagged packets to pass for the multicast VLAN. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.

---

**Table 358** Configure multicast VLAN on the Layer 3 switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the port as a trunk or hybrid port</td>
<td>`port link-type { trunk</td>
<td>hybrid }`</td>
</tr>
<tr>
<td>Specify the VLANs to be allowed to pass the Ethernet port</td>
<td>`port hybrid vlan vlan-id-list { tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td></td>
<td><code>port trunk permit vlan vlan-list</code></td>
<td>The multicast VLAN defined on the Layer 2 switch must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.</td>
</tr>
</tbody>
</table>

---

**Table 359** Configure multicast VLAN on the Layer 2 switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td><code>igmp-snooping enable</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td><code>vlan vlan-id</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td><code>igmp-snooping enable</code></td>
<td>Required</td>
</tr>
<tr>
<td>Enable multicast VLAN</td>
<td><code>service-type multicast</code></td>
<td>Required</td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view for the Layer 3 switch</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Define the port as a trunk or hybrid port</td>
<td>`port link-type { trunk</td>
<td>hybrid }`</td>
</tr>
<tr>
<td>Specify the VLANs to be allowed to pass the Ethernet port</td>
<td>`port hybrid vlan vlan-id-list { tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td></td>
<td><code>port trunk permit vlan vlan-list</code></td>
<td>The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.</td>
</tr>
</tbody>
</table>

---

Enter Ethernet port view for a user device

Define the port as a hybrid port

Specify the VLANs to be allowed to pass the port

---

Enter Ethernet port view for a user device

Define the port as a hybrid port

Specify the VLANs to be allowed to pass the port

---

The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
The multicast VLAN function and the VLAN mapping function cannot be configured at the same time.

Displaying and Maintaining IGMP Snooping

After the configuration above, you can execute the following display commands in any view to verify the configuration by checking the displayed information.

You can execute the reset command in user view to clear the statistics information about IGMP Snooping.

### Table 360 Display and maintain IGMP Snooping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current IGMP Snooping configuration</td>
<td>display igmp-snooping configuration</td>
<td>You can execute the display commands in any view.</td>
</tr>
<tr>
<td>Display IGMP Snooping message statistics</td>
<td>display igmp-snooping statistics</td>
<td></td>
</tr>
<tr>
<td>Display the information about IP and MAC multicast groups in one or all VLANs</td>
<td>display igmp-snooping group [ vlan vlanid ]</td>
<td></td>
</tr>
<tr>
<td>Clear IGMP Snooping statistics</td>
<td>reset igmp-snooping statistics</td>
<td>You can execute the reset command in user view.</td>
</tr>
</tbody>
</table>

IGMP Snooping Configuration Examples

The examples in this section reflect that of the Switch 5500. If you are using a Switch 5500G, GigabitEthernet displays rather than Ethernet.

Configuring IGMP Snooping

Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP snooping on Layer 2 switches.

- As shown in Figure 134, Router A connects to a multicast source (Source) through Ethernet 1/0/2, and to Switch A through Ethernet 1/0/1.
- Run PIM-DM and IGMP on Router A. Run IGMP snooping on Switch A. Router A acts as the IGMP querier.
- The multicast source sends multicast data to the multicast group 224.1.1.1. Host A and Host B are receivers of the multicast group 224.1.1.1.
Network diagram

Figure 134  Network diagram for IGMP Snooping configuration

Configuration procedure

1  Configure the IP address of each interface

Configure an IP address and subnet mask for each interface as per Figure 134. The detailed configuration steps are omitted.

2  Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface Ethernet 1/0/1
[RouterA-Ethernet1/0/1] igmp enable
[RouterA-Ethernet1/0/1] pim dm
[RouterA-Ethernet1/0/1] quit
[RouterA] interface Ethernet 1/0/2
[RouterA-Ethernet1/0/2] pim dm
[RouterA-Ethernet1/0/2] quit
```

3  Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
   Enable IGMP-Snooping ok.

# Create VLAN 100, assign Ethernet1/0/1 through Ethernet 1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/4
```
4 Verify the configuration

# View the detailed information of the multicast group in VLAN 100 on Switch A.

```text
<SwitchA> display igmp-snooping group vlan100
Total 1 IP Group(s).
Total 1 MAC Group(s).
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 MAC Group(s).
  Static Router port(s):
    Ethernet1/0/1
  Dynamic Router port(s):
    Ethernet1/0/3    Ethernet1/0/4
  IP group(s): the following ip group(s) match to one mac group.
    IP group address: 224.1.1.1
    Static host port(s):
    Dynamic host port(s):
    Dynamic Router port(s):
      Ethernet1/0/2    Ethernet1/0/4
  MAC group(s):
    MAC group address: 0100-5e01-0101
    Host port(s): Ethernet1/0/3    Ethernet1/0/4
```

As shown above, the multicast group 224.1.1.1 has been registered on Switch A, with the dynamic router port Ethernet 1/0/1 and dynamic member ports Ethernet 1/0/3 and Ethernet 1/0/4. This means that Host A and Host B have joined the multicast group 224.1.1.1.

### Configuring Multicast VLAN

**Network requirements**

As shown in Figure 135, Workstation is a multicast source. Switch A forwards multicast data from the multicast source. A Layer 2 switch, Switch B forwards the multicast data to the end users Host A and Host B.

Table 361 describes the network devices involved in this example and the configurations you should make on them.

### Table 361  Network devices and their configurations

<table>
<thead>
<tr>
<th>Device</th>
<th>Device description</th>
<th>Networking description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Layer 3 switch</td>
<td>The interface IP address of VLAN 20 is 168.10.1.1. Ethernet 1/0/1 is connected to the workstation and belongs to VLAN 20. The interface IP address of VLAN 10 is 168.10.2.1. Ethernet 1/0/10 belongs to VLAN 10. Ethernet 1/0/10 is connected to Switch B.</td>
</tr>
</tbody>
</table>
In this configuration example, you need to configure the ports that connect Switch A and Switch B to each other as hybrid ports. The following text describes the configuration details. You can also configure these ports as trunk ports. The configuration procedure is omitted here. For details, see “Configuring Multicast VLAN” on page 468.

Configure a multicast VLAN, so that users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

Network diagram

Table 361  Network devices and their configurations

<table>
<thead>
<tr>
<th>Device</th>
<th>Device description</th>
<th>Networking description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch B</td>
<td>Layer 2 switch</td>
<td>VLAN 2 contains Ethernet 1/0/1 and VLAN 3 contains Ethernet 1/0/2. The default VLANs of Ethernet 1/0/1 and Ethernet 1/0/2 are VLAN 2 and VLAN 3 respectively. VLAN 10 contains Ethernet 1/0/10, Ethernet 1/0/1, and Ethernet 1/0/2. Ethernet 1/0/10 is connected to Switch A. VLAN 10 is a multicast VLAN. Ethernet 1/0/1 sends untagged packets for VLAN 2 and VLAN 10. Ethernet 1/0/2 sends untagged packets for VLAN 3 and VLAN 10.</td>
</tr>
<tr>
<td>Host A</td>
<td>User 1</td>
<td>PC 1 is connected to Ethernet 1/0/1 on Host A.</td>
</tr>
<tr>
<td>Host B</td>
<td>User 2</td>
<td>PC 2 is connected to Ethernet 1/0/2 on Host B.</td>
</tr>
</tbody>
</table>
**Configuration procedure**

The following configuration is based on the prerequisite that the devices are properly connected and all the required IP addresses are already configured.

1) Configure Switch A:

   # Set the interface IP address of VLAN 20 to 168.10.1.1 and enable PIM DM on the VLAN interface.

   <SwitchA> system-view
   [SwitchA] multicast routing-enable
   [SwitchA] vlan 20
   [SwitchA-vlan20] port Ethernet 1/0/1
   [SwitchA-vlan20] quit
   [SwitchA] interface Vlan-interface 20
   [SwitchA-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
   [SwitchA-Vlan-interface20] pim dm
   [SwitchA-Vlan-interface20] quit

   # Configure VLAN 10.

   [SwitchA] vlan 10
   [SwitchA-vlan10] quit

   # # Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 10, and configure the port to forward tagged packets for VLAN 10.

   [SwitchA] interface Ethernet 1/0/10
   [SwitchA-Ethernet1/0/10] port link-type hybrid
   [SwitchA-Ethernet1/0/10] port hybrid vlan 10 tagged
   [SwitchA-Ethernet1/0/10] quit

   # Configure the interface IP address of VLAN 10 as 168.10.2.1, and enable PIM-DM and IGMP.

   [SwitchA] interface Vlan-interface 10
   [SwitchA-Vlan-interface10] ip address 168.10.2.1 255.255.255.0
   [SwitchA-Vlan-interface10] igmp enable
   [SwitchA-Vlan-interface10] pim dm

1) Configure Switch B:

   # Enable the IGMP Snooping feature on Switch B.

   <SwitchB> system-view
   [SwitchB] igmp-snooping enable

   # Create VLAN 2, VLAN 3 and VLAN 10, configure VLAN 10 as the multicast VLAN, and then enable IGMP Snooping on it.

   [SwitchB] vlan 2 to 3
   Please wait.... Done.
   [SwitchB] vlan 10
   [SwitchB-vlan10] service-type multicast
   [SwitchB-vlan10] igmp-snooping enable
   [SwitchB-vlan10] quit
# Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to forward tagged packets for VLAN 2, VLAN 3, and VLAN 10.

```
[SwitchB] interface Ethernet 1/0/10
[SwitchB-Ethernet1/0/10] port link-type hybrid
[SwitchB-Ethernet1/0/10] port hybrid vlan2 3 10 tagged
[SwitchB-Ethernet1/0/10] quit
```

# Define Ethernet 1/0/1 as a hybrid port, add the port to VLAN 2 and VLAN 10, configure the port to forward untagged packets for VLAN 2 and VLAN 10, and set VLAN 2 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type hybrid
[SwitchB-Ethernet1/0/1] port hybrid vlan 2 10 untagged
[SwitchB-Ethernet1/0/1] port hybrid pvid vlan 2
[SwitchB-Ethernet1/0/1] quit
```

# Define Ethernet 1/0/2 as a hybrid port, add the port to VLAN 3 and VLAN 10, configure the port to forward untagged packets for VLAN 3 and VLAN 10, and set VLAN 3 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type hybrid
[SwitchB-Ethernet1/0/2] port hybrid vlan 3 10 untagged
[SwitchB-Ethernet1/0/2] port hybrid pvid vlan 3
[SwitchB-Ethernet1/0/2] quit
```

---

**Troubleshooting IGMP Snooping**

**Symptom:** Multicast function does not work on the switch.

**Solution:**

Possible reasons are:

1. IGMP Snooping is not enabled.
   - Use the `display current-configuration` command to check the status of IGMP Snooping.
   - Use the `igmp-snooping enable` command in both system view and VLAN view to enable it both globally and on the corresponding VLAN at the same time. If it is only disabled on the corresponding VLAN, use the `igmp-snooping enable` command in VLAN view only to enable it on the corresponding VLAN.

2. Multicast forwarding table set up by IGMP Snooping is wrong.
   - Use the `display igmp-snooping group` command to check if the multicast groups are expected ones.
   - If the multicast group set up by IGMP Snooping is not correct, contact your technical support personnel.
**802.1x Configuration**

**Introduction to 802.1x**

The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those fail to pass the authentication are denied when accessing the LAN.

**Architecture of 802.1x Authentication**

As shown in Figure 136, 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

Figure 136  Architecture of 802.1x authentication

- The supplicant system is an entity residing at one end of a LAN segment and is authenticated by the authenticator system at the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is triggered when a user launches client program on the supplicant system. Note that the client program must support the Extensible Authentication Protocol over LAN (EAPoL).

- The authenticator system is another entity residing at one end of a LAN segment. It authenticates the connected supplicant systems. The authenticator system is usually an 802.1x-supported network device (such as a 3Com series switch). It provides the port (physical or logical) for the supplicant system to access the LAN.
The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server, the authentication server system serves to perform Authentication, Authorization, and Accounting (AAA) services to users. It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and the Access Control List (ACLs) applied.

The four basic concepts related to the above three entities are PAE, controlled port and uncontrolled port, the valid direction of a controlled port and the way a port is controlled.

**PAE**
A Port Access Entity (PAE) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

- The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the status (authorized/unauthorized) of the controlled ports according to the authentication result.
- The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

**Controlled port and uncontrolled port**
The authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

**The valid direction of a controlled port**
When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

**The way a port is controlled**
A port of a 3Com series switch can be controlled in the following two ways.

- Port-based authentication. When a port is controlled in this way, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses the Extensible Authentication Protocol (EAP) to exchange information between the supplicant system and the authentication server.

**Figure 137** The mechanism of an 802.1x authentication system

- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP) protocol packets.
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

Encapsulation of EAPoL Messages

**The format of an EAPoL packet**

EAPoL is a packet encapsulation format defined in 802.1x. To enable EAP protocol packets to be transmitted between supplicant systems and authenticator systems through LANs, EAP protocol packets are encapsulated in EAPoL format. The following figure illustrates the structure of an EAPoL packet.

**Figure 138** The format of an EAPoL packet

In an EAPoL packet:

- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
The Type field can be one of the following:
- 00: Indicates that the packet is an EAP-packet, which carries authentication information.
- 01: Indicates that the packet is an EAPoL-start packet, which initiates the authentication.
- 02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.
- 03: Indicates that the packet is an EAPoL-key packet, which carries key information.
- 04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of Alerting Standards Forum (ASF).

The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.

The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP-packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

The format of an EAP packet

For an EAPoL packet with the value of the Type field being EAP-packet, its Packet body field is an EAP packet, whose format is illustrated in Figure 139.

**Figure 139** The format of an EAP packet

```
<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

In an EAP packet:
- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.
- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field carries the EAP packet whose format differs from the Code field.

A Success or Failure packet does not contain the Data field, so the Length field of it is 4.
Figure 140 shows the format of the Data field of a Request packet or a Response packet.

**Figure 140** The format of the Data field of a Request packet or a Response packet

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type data</td>
<td></td>
</tr>
</tbody>
</table>

- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.

- The Type Data field differs with types of Request and Response packets.

**Newly added fields for EAP authentication**

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication. (Refer to “RADIUS Configuration Task List” on page 527 for information about the format of a RADIUS protocol packet.)

The EAP-message field, whose format is shown in Figure 141, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field is 79.

**Figure 141** The format of an EAP-message field

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>15</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Length</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>

The Message-authenticator field, whose format is shown in Figure 142, is used to prevent unauthorized interception to access requesting packets during authentications using CHAP, EAP, and so on. A packet with the EAP-message field must also have the Message-authenticator field. Otherwise, the packet is regarded as invalid and is discarded.

**Figure 142** The format of an Message-authenticator field

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>18 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Length</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>

**802.1x Authentication Procedure**

The Switch 5500 can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

**EAP relay mode**

This mode is defined in 802.1x. In this mode, EAP-packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server
support the two newly-added fields: the EAP message field (with a value of 79) and the Message-authenticator field (with a value of 80).

Four authentication ways, namely EAP-MD5, EAP-TLS (transport layer security), EAP-TTLS (tunneled transport layer security), and Protected Extensible Authentication Protocol (PEAP), are available in the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.

- EAP-TLS allows the supplicant system and the RADIUS server to check each other’s security certificate and authenticate each other’s identity, guaranteeing that data is transferred to the right destination and preventing data from being intercepted.

- EAP-TTLS is a kind of extended EAP-TLS. EAP-TLS implements bidirectional authentication between the client and authentication server. EAP-TTLS transmit message using a tunnel established using TLS.

- PEAP creates and uses TLS security channels to ensure data integrity and then performs new EAP negotiations to verify supplicant systems.

Figure 143 describes the basic EAP-MD5 authentication procedure.
The detailed procedure is as follows:

- A supplicant system launches an 802.1x client to initiate an access request by sending an EAPoL-start packet to the switch, with its user name and password provided. The 802.1x client program then forwards the packet to the switch to start the authentication process.

- Upon receiving the authentication request packet, the switch sends an EAP-request/identity packet to ask the 802.1x client for the user name.

- The 802.1x client responds by sending an EAP-response/identity packet to the switch with the user name contained in it. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.

- Upon receiving the packet from the switch, the RADIUS server retrieves the user name from the packet, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS access-challenge packet. The switch then sends the key to the 802.1x client.
Upon receiving the key (encapsulated in an EAP-request/MD5 challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the switch. (Normally, the encryption is irreversible.)

The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the switch to indicate that the supplicant system is authenticated.

The switch changes the state of the corresponding port to accepted state to allow the supplicant system to access the network.

The supplicant system can also terminate the authenticated state by sending EAPoL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you can simply enable the EAP relay mode by using the `dot1x authentication-method eap` command.

EAP terminating mode

In this mode, EAP packet transmission is terminated at authenticator systems and the EAP packets are converted to RADIUS packets. Authentication and accounting are carried out through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. Figure 144 illustrates the authentication procedure (assuming that CHAP is employed between the switch and the RADIUS server).
The authentication procedure in EAP terminating mode is the same as that in the EAP relay mode except that the randomly-generated key in the EAP terminating mode is generated by the switch, and that it is the switch that sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication.

**Timers Used in 802.1x**

In 802.1x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way.

- **Handshake timer** *(handshake-period)*. This timer sets the handshake period and is triggered after a supplicant system passes the authentication. It sets the interval for a switch to send handshake request packets to online users. You can set the maximum number of transmission attempts by using the `dot1x retry` command. An online user is considered offline when the switch has not received any response packets after the maximum number of handshake request transmission attempts is reached.

- **Quiet-period timer** *(quiet-period)*. This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system.
Re-authentication timer (\texttt{reauth-period}). The switch initiates 802.1x re-authentication at the interval set by the re-authentication timer.

RADIUS server timer (\texttt{server-timeout}). This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, the switch sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.

Supplicant system timer (\texttt{supp-timeout}). This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the switch does not receive the response from the supplicant system when this timer times out.

Transmission timer (\texttt{tx-period}). This timer sets the tx-period and is triggered by the switch in two cases. The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client who cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets.

Client version request timer (\texttt{ver-period}). This timer sets the version period and is triggered after a switch sends a version request packet. The switch sends another version request packet if it does receive version response packets from the supplicant system when the timer expires.

802.1x Implementation on a Switch 5500

In addition to the earlier mentioned 802.1x features, the Switch 5500 is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, and so on (This function needs the cooperation of a CAMS server.)
- Checking client version
- The Guest VLAN function

\textit{3Com's CAMS Server is a service management system used to manage networks and to secure networks and user information. With the cooperation of other networking devices (such as switches) in the network, a CAMS server can implement the AAA functions and rights management.}

Checking the supplicant system

The Switch 5500 checks:

- Supplicant systems logging on through proxies
- Supplicant systems logging on through IE proxies
- Whether or not a supplicant system logs in through more than one network adapters (that is, whether or not more than one network adapters are active in a supplicant system when the supplicant system logs in).

In response to any of the three cases, a switch can optionally take the following measures:
- Only disconnects the supplicant system but sends no Trap packets;
- Sends Trap packets without disconnecting the supplicant system.

This function needs the cooperation of 802.1x client and a CAMS server.

- The 802.1x client needs to be capable of detecting multiple network adapters, proxies, and IE proxies.
- The CAMS server is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client program allows use of multiple network adapters, proxies, and IE proxies. In this case, if the CAMS server is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

- The client-checking function needs the support of 3Com’s 802.1x client program.

- To implement the proxy detecting function, you need to enable the function on both the 802.1x client program and the CAMS server in addition to enabling the client version detecting function on the switch by using the `dot1x version-check` command.

**Checking the client version**

With the 802.1x client version-checking function enabled, a switch checks the version and validity of an 802.1x client to prevent unauthorized users or users with earlier versions of 802.1x client from logging in.

This function makes the switch to send version-requesting packets again if the 802.1x client fails to send version-reply packet to the switch when the version-checking timer times out.

- The 802.1x client version-checking function needs the support of 3Com’s 802.1x client program.

**The Guest VLAN function**

The Guest VLAN function enables supplicant systems that are not authenticated to access network resources in a restrained way.

The Guest VLAN function enables supplicant systems that do not have 802.1x client installed to access specific network resources. It also enables supplicant systems that are not authenticated to upgrade their 802.1x client programs.

With this function enabled:

- The switch sends authentication triggering request (EAP-Request/Identity) packets to all the 802.1x-enabled ports.
- After the maximum number retries have been made and there are still ports that have not sent any response back, the switch will then add these ports to the Guest VLAN.
Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated when accessing external resources.

Normally, the Guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to “Introduction to AAA Services” on page 510 for detailed information about the dynamic VLAN delivery function.

**Enabling 802.1x re-authentication**

802.1x re-authentication is timer-triggered or packet-triggered. It re-authenticates users who successfully pass authentication. With 802.1x re-authentication enabled, the switch can monitor the connection status of users periodically. If the switch receives no re-authentication response from a user in a period of time, it tears down the connection to the user. To connect to the switch again, the user needs to initiate 802.1x authentication with the client software again.

- **When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.**

- **An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.**

**Figure 145** 802.1x re-authentication

802.1x re-authentication can be enabled in one of the following two ways:

- The RADIUS server triggers the switch to perform 802.1x re-authentication for users. The RADIUS server sends the switch an Access-Accept packet with the Termination-Action field of 1. Upon receiving the packet, the switch re-authenticates users periodically.
You enable 802.1x re-authentication on the switch. With the 802.1x re-authentication enabled, the switch re-authenticates users periodically.

**802.1x Re-authentication will Fail if a CAMS Server is Used and Configured to Perform Authentication but Not Accounting.** This is because a CAMS server establishes a user session after it begins to perform accounting. Therefore, to enable 802.1x re-authentication, do not configure the `accounting none` command in the domain. This restriction does not apply to other types of servers.

---

**802.1x Configuration Overview**

802.1x provides a solution for authenticating users. To implement this solution, you need to execute 802.1x-related commands. You also need to configure AAA schemes on switches and specify the authentication scheme (RADIUS, HWTACACS or local authentication scheme).

![802.1x Configuration Diagram](image)

- 802.1x users use domain names to associate with the ISP domains configured on switches.
- Configure the AAA scheme (a local authentication scheme or a RADIUS scheme) to be adopted in the ISP domain.
- If you opt to adopt a local authentication scheme, you need to configure user names and passwords manually on the switch. Users can pass the authentication through 802.1x client if they provide user names and passwords that match those configured on the switch.
- If you specify to adopt the RADIUS scheme, the supplicant systems are authenticated by a remote RADIUS server. In this case, you need to configure user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the switch.
- You can also specify to adopt the RADIUS authentication scheme, with a local authentication scheme as a backup. In this case, the local authentication scheme is adopted when the RADIUS server or the TACACS server fails.

Refer to “AAA Configuration” on page 519 for detailed information about AAA scheme configuration.

---

**Basic 802.1x Configuration**

<table>
<thead>
<tr>
<th>Configuration Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ISP domain and the AAA scheme to be adopted. You can specify a RADIUS scheme, a HWTACACS scheme, or a local scheme.</td>
</tr>
<tr>
<td>Ensure that the service type is configured as <code>lan-access</code> (by using the <code>service-type</code> command) if local authentication scheme is adopted.</td>
</tr>
</tbody>
</table>
### Configuring Basic 802.1x Functions

#### Table 362  Configure basic 802.1x functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable 802.1x globally</td>
<td><code>dot1x</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, 802.1x is disabled globally.</td>
</tr>
<tr>
<td>Enable 802.1x for specified ports</td>
<td><code>dot1x interface interface-list</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td><code>interface interface-type interface-number</code></td>
<td>By default, 802.1x is disabled on all ports.</td>
</tr>
<tr>
<td></td>
<td><code>dot1x</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>quit</code></td>
<td></td>
</tr>
<tr>
<td>Set port access control mode for specified ports</td>
<td>`dot1x port-control { authorized-force</td>
<td>unauthorized-force</td>
</tr>
<tr>
<td></td>
<td>`dot1x port-control { authorized-force</td>
<td>unauthorized-force</td>
</tr>
<tr>
<td></td>
<td><code>quit</code></td>
<td></td>
</tr>
<tr>
<td>Set port access method for specified ports</td>
<td>`dot1x port-method { macbased</td>
<td>portbased } [ interface interface-list ] interface interface-type interface-number`</td>
</tr>
<tr>
<td></td>
<td>`dot1x port-method { macbased</td>
<td>portbased }`</td>
</tr>
<tr>
<td></td>
<td><code>quit</code></td>
<td></td>
</tr>
<tr>
<td>Set authentication method for 802.1x users</td>
<td>`dot1x authentication-method { chap</td>
<td>pap</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a switch performs CHAP authentication in EAP terminating mode.</td>
</tr>
<tr>
<td>Enable online user handshaking</td>
<td><code>dot1x handshake enable</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, online user handshaking is enabled.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.

- The settings of 802.1x and MAC address learning limit are mutually exclusive. Enabling 802.1x on a port will prevent you from setting the limit on MAC address learning on the port and vice versa.

- The settings of 802.1x and aggregation group member are mutually exclusive. Enabling 802.1x on a port will prevent you from adding the port to an aggregation group and vice versa.

- When a device operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
With the support of the 3Com-proprietary client, handshaking packets are used to test whether or not a user is online.

As clients that are not of 3Com do not support the online user handshaking function, switches cannot receive handshaking acknowledgement packets from them in handshaking periods. To prevent users being falsely considered offline, you need to disable the online user handshaking function in this case.

The handshaking packet protection function requires the cooperation of the client and the authentication server. If either of the two ends does not support the function, you need to disable it on the other one.

---

### Table 363 Configure 802.1x timers and the maximum number of users

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Set the maximum number of concurrent on-line users for specified ports</td>
<td><strong>dot1x max-user user-number</strong></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>interface</strong> interface-list</td>
<td>By default, a port can accommodate up to 256 users at a time.</td>
</tr>
<tr>
<td></td>
<td><strong>interface</strong> interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>dot1x max-user user-number</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>quit</strong></td>
<td></td>
</tr>
<tr>
<td>Set the maximum retry times to send request packets</td>
<td><strong>dot1x retry max-retry-value</strong></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>dot1x timer</strong> {</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td><strong>handshake-period</strong> handshake-period-value</td>
<td>The settings of 802.1x timers are as follows.</td>
</tr>
<tr>
<td></td>
<td><strong>quiet-period</strong> quiet-period-value</td>
<td>- handshake-period-value: 15 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>server-timeout</strong> server-timeout-value</td>
<td>- quiet-period-value: 60 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>supp-timeout</strong> supp-timeout-value</td>
<td>- server-timeout-value: 100 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>tx-period</strong> tx-period-value</td>
<td>- supp-timeout-value: 30 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>ver-period</strong> ver-period-value }</td>
<td>- tx-period-value: 30 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>dot1x quiet-period</strong></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the quiet-period timer is disabled.</td>
</tr>
</tbody>
</table>

---

As for the **dot1x max-user** command, if you execute it in system view without specifying the interface-list argument, the command applies to all ports. You
can also use this command in port view. In this case, this command applies to the current port only and the interface-list argument is not needed.

- As for the configuration of 802.1x timers, the default values are recommended.

---

### Advanced 802.1x Configuration

Advanced 802.1x configurations, as listed below, are all optional.

- Configuration concerning CAMS, including multiple network adapters detecting, proxy detecting, and so on.
- Client version checking configuration
- DHCP-triggered authentication
- Guest VLAN configuration
- 802.1x re-authentication configuration
- Configuration of the 802.1x re-authentication timer

You need to configure basic 802.1x functions before configuring 802.1x features.

---

### Configuring Proxy Checking

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable proxy checking</td>
<td>`dot1x supp-proxy-check { logoff</td>
<td>trap }`</td>
</tr>
</tbody>
</table>
| function globally          |                                              | By default, the 802.1x proxy checking function is globally disabled.
| Enable proxy checking      | `dot1x supp-proxy-check { logoff | trap } [ interface interface-list ]` | Required                        |
| for a port/specifed ports  | In system view `interface interface-type interface-number` | By default, the 802.1x proxy checking is disabled on a port. |
|                            | In port view `dot1x supp-proxy-check { logoff | trap }` |                                  |
|                            | `quit`                                       |                                  |

- The proxy checking function needs the cooperation of 3Com's 802.1x client (iNode) program.
- The proxy checking function depends on the online user handshaking function. To enable the proxy detecting function, you need to enable the online user handshaking function first.
- The configuration listed in Table 364 takes effect only when it is performed on CAMS as well as on the switch. In addition, the client version checking function needs to be enabled on the switch too (by using the `dot1x version-check` command).
Configuring Client
Version Checking

Table 365  Configure client version checking

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable 802.1x client version</td>
<td>dot1x version-check [interface interface-list]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>dot1x version-check [interface interface-type]</td>
<td>By default, 802.1x client version checking is disabled on a port.</td>
</tr>
<tr>
<td></td>
<td>[interface interface-number]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of retries to send version checking request packets</td>
<td>dot1x retry-version-max max-retry-version-value</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the maximum number of retries to send version checking request packets is 3.</td>
</tr>
<tr>
<td>Set the client version checking period timer</td>
<td>dot1x timer ver-period ver-period-value</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the timer is set to 30 seconds.</td>
</tr>
</tbody>
</table>

As for the dot1x version-user command, if you execute it in system view without specifying the interface-list argument, the command applies to all ports. You can also execute this command in port view. In this case, this command applies to the current port only and the interface-list argument is not needed.

Enabling DHCP-triggered Authentication

After performing the following configuration, 802.1X allows running DHCP on access users, and users are authenticated when they apply for dynamic IP addresses through DHCP.

Table 366  Enable DHCP-triggered authentication

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable DHCP-triggered authentication</td>
<td>dot1x dhcp-launch</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, DHCP-triggered authentication is disabled.</td>
</tr>
</tbody>
</table>

Configuring Guest VLAN

Table 367  Configure Guest VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure port access method</td>
<td>dot1x port-method portbased</td>
<td>Required</td>
</tr>
<tr>
<td>Enable the Guest VLAN function</td>
<td>dot1x guest-vlan vlan-id [interface interface-list]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>[interface interface-type interface-number]</td>
<td>By default, the Guest VLAN function is disabled.</td>
</tr>
<tr>
<td></td>
<td>quit</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 40: 802.1X CONFIGURATION

CAUTION:

■ The Guest VLAN function is available only when the switch operates in the port-based authentication mode.

■ Only one Guest VLAN can be configured for each switch.

■ The Guest VLAN function cannot be implemented if you configure the `dot1x dhcp-launch` command on the switch to enable DHCP-triggered authentication. This is because the switch does not send authentication packets in that case.

Configuring 802.1x Re-Authentication

Table 368 Enable 802.1x re-authentication

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable 802.1x re-authentication on port(s)</td>
<td><code>dot1x re-authenticate [interface interface-list ]</code></td>
<td>Required</td>
</tr>
<tr>
<td>In system view</td>
<td></td>
<td>By default, 802.1x re-authentication is disabled on a port.</td>
</tr>
<tr>
<td>In port view</td>
<td><code>dot1x re-authenticate</code></td>
<td></td>
</tr>
</tbody>
</table>

■ To enable 802.1x re-authentication on a port, you must first enable 802.1x globally and on the port.

■ When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.

■ An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.

Configuring the 802.1x Re-Authentication Timer

After 802.1x re-authentication is enabled on the switch, the switch determines the re-authentication interval in one of the following two ways:

1. The switch uses the value of the Session-timeout attribute field of the Access-Accept packet sent by the RADIUS server as the re-authentication interval.

2. The switch uses the value configured with the `dot1x timer reauth-period` command as the re-authentication interval for access users.

Note the following:

During re-authentication, the switch always uses the latest re-authentication interval configured, no matter which of the above-mentioned two ways is used to determine the re-authentication interval. For example, if you configure a re-authentication interval on the switch and the switch receives an Access-Accept packet whose Termination-Action attribute field is 1, the switch will ultimately use the value of the Session-timeout attribute field as the re-authentication interval.

The following introduces how to configure the 802.1x re-authentication timer on the switch.
After performing the above configurations, you can display and verify the 802.1x-related configuration by executing the `display` command in any view.

You can clear 802.1x-related statistics information by executing the `reset` command in user view.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure a re-authentication interval</td>
<td><code>dot1x timer reauth-period reauth-period-value</code></td>
<td>Optional By default, the re-authentication interval is 3,600 seconds.</td>
</tr>
</tbody>
</table>

### Network requirements

- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC address-based access control mode.

- All supplicant systems that pass the authentication belong to the default domain named `aabbcc.net`. The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes.

- The switch is connected to a server comprising of two RADIUS servers whose IP addresses are 10.11.1.1 and 10.11.1.2. The RADIUS server with an IP address of 10.11.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and primary accounting server. The password for the switch and the authentication RADIUS servers to exchange message is `name`. And the password for the switch and the accounting RADIUS servers to exchange message is `money`. The switch sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds, with the maximum number of retries of 5. And the switch sends a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated.
The user name and password for local 802.1x authentication are `localuser` and `localpass` (in plain text) respectively. The idle disconnecting function is enabled.

### Network diagram

**Figure 147** Network diagram for AAA configuration with 802.1x and RADIUS enabled

![Network Diagram](image)

### Configuration procedure

Following configuration covers the major AAA/RADIUS configuration commands. Refer to “AAA Configuration” on page 519 for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

1. **# Enable 802.1x globally.**

   ```
   <5500> system-view
   System View: return to User View with Ctrl+Z.
   [5500] dot1x
   ```

2. **# Enable 802.1x on Ethernet 1/0/1.**

   ```
   [5500] dot1x interface Ethernet 1/0/1
   ```

3. **# Set the access control method to MAC-based (This operation can be omitted, as MAC-based is the default).**

   ```
   [5500] dot1x port-method macbased interface Ethernet 1/0/1
   ```

4. **# Create a RADIUS scheme named `radius1` and enter RADIUS scheme view.**

   ```
   [5500] radius scheme radius1
   ```

5. **# Assign IP addresses to the primary authentication and accounting RADIUS servers.**

   ```
   [5500-radius-radius1] primary authentication 10.11.1.1
   [5500-radius-radius1] primary accounting 10.11.1.2
   ```

6. **# Assign IP addresses to the secondary authentication and accounting RADIUS server.**

   ```
   [5500-radius-radius1] secondary authentication 10.11.1.2
   [5500-radius-radius1] secondary accounting 10.11.1.1
   ```
# Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[5500-radius-radius1] key authentication name
```

# Set the password for the switch and the accounting RADIUS servers to exchange messages.

```
[5500-radius-radius1] key accounting money
```

# Set the interval and the number of the retries for the switch to send packets to the RADIUS servers.

```
[5500-radius-radius1] timer 5
[5500-radius-radius1] retry 5
```

# Set the timer for the switch to send real-time accounting packets to the RADIUS servers.

```
[5500-radius-radius1] timer realtime-accounting 15
```

# Configure to send the user name to the RADIUS server with the domain name truncated.

```
[5500-radius-radius1] user-name-format without-domain
[5500-radius-radius1] quit
```

# Create the domain named **aabbcc.net** and enter its view.

```
[5500] domain enable aabbcc.net
```

# Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS server is invalid, specify to adopt the local authentication scheme.

```
[5500-isp-aabbcc.net] scheme radius-scheme radius1 local
```

# Specify the maximum number of users the user domain can accommodate to 30.

```
[5500-isp-aabbcc.net] access-limit enable 30
```

# Enable the idle disconnecting function and set the related parameters.

```
[5500-isp-aabbcc.net] idle-cut enable 20 2000
[5500-isp-aabbcc.net] quit
```

# Set the default user domain to be **aabbcc.net**.

```
[5500] domain default enable aabbcc.net
```

# Create a local access user account.

```
[5500] local-user localuser
[5500-luser-localuser] service-type lan-access
[5500-luser-localuser] password simple localpass
```
Quick EAD Deployment

Introduction to Quick EAD Deployment

As an integrated solution, an Endpoint Admission Defense (EAD) solution can improve the overall defense power of a network. In real applications, however, deploying EAD clients proves to be time consuming and inconvenient.

To address the issue, the Switch 5500 Family provides the forcible deployment of EAD clients with 802.1x authentication, easing the work of EAD client deployment.

Quick EAD deployment is achieved with the two functions: restricted access and HTTP redirection.

Restricted access

Before passing 802.1x authentication, a user is restricted (through ACLs) to a specific range of IP addresses or a specific server. Services like EAD client upgrading/download and dynamic address assignment are available on the specific server.

HTTP redirection

In the HTTP redirection approach, when the terminal users that have not passed 802.1x authentication access the Internet through Internet Explorer, they are redirected to a predefined URL for EAD client download.

The two functions ensure that all the users without an EAD client have downloaded and installed one from the specified server themselves before they can access the Internet, thus decreasing the complexity and effort that EAD client deployment may involve.

The quick EAD deployment feature takes effect only when the access control mode of an 802.1x-enabled port is set to auto.

Configuring Quick EAD Deployment

Configuration Prerequisites

- Enable 802.1x on the switch.
- Set the access mode to auto for 802.1x-enabled ports.

Configuration Procedure

Configuring a free IP range

A free IP range is an IP range that users can access before passing 802.1x authentication.
Follow the steps in Table 371 to configure a free IP range:

**Table 371  Configuring a free IP range**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure the URL for HTTP redirection</td>
<td>dot1x url url-string</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a free IP range</td>
<td>dot1x free-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>mask-address</td>
<td>By default, no free IP range is configured.</td>
</tr>
<tr>
<td></td>
<td>mask-length</td>
<td></td>
</tr>
</tbody>
</table>

**Caution:**

- You must configure the URL for HTTP redirection before configuring a free IP range. A URL must start with http:// and the segment where the URL resides must be in the free IP range. Otherwise, the redirection function cannot take effect.
- You must disable the DHCP-triggered authentication function of 802.1x before configuring a free IP range.
- With dot1x enabled but quick EAD deployment disabled, users cannot access the DHCP server if they fail 802.1x authentication. With quick EAD deployment enabled, users can obtain IP addresses dynamically before passing authentication if the IP address of the DHCP server is in the free IP range.
- The quick EAD deployment function applies to only ports with the access control mode set to auto through the dot1x port-control command.
- At present, 802.1x is the only access approach that supports quick EAD deployment.
- Currently, the quick EAD deployment function does not support port security. The configured free IP range cannot take effect if you enable port security.

**Setting the ACL timeout period**

The quick EAD deployment function depends on ACLs in restricting access of users failing authentication. Each online user that has not passed authentication occupies a certain amount of ACL resources. After a user passes authentication, the occupied ACL resources will be released. When a large number of users log in but cannot pass authentication, the switch may run out of ACL resources, preventing other users from logging in. A timer called ACL timer is designed to solve this problem.

You can control the usage of ACL resources by setting the ACL timer. The ACL timer starts once a user gets online. If the user has not passed authentication when the ACL timer expires, the occupied ACL resources are released for other users to use. When a tremendous of access requests are present, you can decrease the timeout period of the ACL timer appropriately for higher utilization of ACL resources.
Follow the steps in Table 372 to configure the ACL timer:

**Table 372  Setting the ACL timeout period**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Set the ACL timer</td>
<td><code>dot1x timer acl-timeout</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td><code>acl-timeout-value</code></td>
<td>By default, the ACL timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>period is 30 minutes.</td>
</tr>
</tbody>
</table>

Follow the steps in Table 373 to display and maintain Quick EAD deployment.

**Table 373  Displaying and Maintaining Quick EAD Deployment**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configuration information about</td>
<td>`display dot1x [sessions</td>
<td>Available in any view</td>
</tr>
<tr>
<td>quick EAD deployment</td>
<td>statistics]`</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>[interface interface-list]</code></td>
<td></td>
</tr>
</tbody>
</table>

**Quick EAD Deployment Configuration Example**

**Network requirements** A user connects to the switch directly. The switch connects to the Web server and the Internet. The user will be redirected to the Web server to download the authentication client and upgrade software when accessing the Internet through IE before passing authentication. After passing authentication, the user can access the Internet.

**Network diagram** Figure 148  Network diagram for quick EAD deployment
CHAPTER 41: QUICK EAD DEPLOYMENT CONFIGURATION

Configuration procedure

Before enabling quick EAD deployment, be sure that:

- The Web server is configured properly.
- The default gateway of the user's PC is configured as the IP address of the connected VLAN interface on the switch.

# Configure the URL for HTTP redirection.

```
<5500> system-view
[5500] dot1x url http://192.168.0.111
```

# Configure a free IP range.

```
[5500] dot1x free-ip 192.168.0.111 24
```

# Set the ACL timer to 10 minutes.

```
[5500] dot1x timer acl-timeout 10
```

# Enable dot1x globally.

```
[5500] dot1x
```

# Enable dot1x for Ethernet 1/0/1.

```
[5500] dot1x interface Ethernet 1/0/1
```

Troubleshooting

**Symptom**

User cannot be redirected to the specified URL server, no matter what URL the user enters in the IE address bar.

**Solution**

- If a user enters an IP address in a format other than the dotted decimal notation, the user may not be redirected. This is related with the operating system used on the PC. In this case, the PC considers the IP address string a name and tries to resolve the name. If the resolution fails, the PC will access a specific website. Generally, this address is not in dotted decimal notation. As a result, the PC cannot receive any ARP response and therefore cannot be redirected. To solve this problem, the user needs to enter an IP address that is not in the free IP range in dotted decimal notation.

- If a user enters an address in the free IP range, the user cannot be redirected. This is because the switch considers that the user wants to access a host in the free IP range, unconcerned about whether this PC exists or not. To solve this problem, the user needs to enter an address not in the free IP range.

- Check that you have configured an IP address in the free IP range for the Web server and a correct URL for redirection, and that the server provides Web services properly.
**Introduction to HABP**

When a switch is configured with the 802.1x function, 802.1x will authenticate and authorize 802.1x-enabled ports and allow only the authorized ports to forward packets. In case a port fails 802.1x authentication and authorization, service packets from and to that port will be blocked, making it impossible to manage the switch attached to the port. The Huawei Authentication Bypass Protocol (HABP) aims at solving this problem.

An HABP packet carries the MAC addresses of the attached switches with it. It can bypass the 802.1x authentications when traveling between HABP-enabled switches, through which management devices can obtain the MAC addresses of the attached switches and thus the management of the attached switches is feasible.

HABP is built on the client-server model. Typically, the HABP server sends HABP requests to the client periodically to collect the MAC address(es) of the attached switch(es). The client responds to the requests, and forwards the HABP requests to the attached switch(es). The HABP server usually runs on the administrative device while the HABP client runs on the attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

**HABP Server Configuration**

With the HABP server launched, a management device sends HABP request packets regularly to the attached switches to collect their MAC addresses. You need also to configure the interval on the management device for an HABP server to send HABP request packets.

**Table 374**  Configure an HABP server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable HABP</td>
<td>hhabp enable</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the current</td>
<td>hhabp server vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td>switch to be an HABP server</td>
<td></td>
<td>By default, HABP is enabled. Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a switch operates as an HABP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>client after you enable HABP on the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you want to use the switch as a management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>switch, you need to configure the switch to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be an HABP server.</td>
</tr>
</tbody>
</table>
HABP Client Configuration

HABP clients reside on switches attached to HABP servers. After you enable HABP for a switch, the switch operates as an HABP client by default. So you only need to enable HABP on a switch to make it an HABP client.

Table 374 Configure an HABP server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the interval to send HABP request packets.</td>
<td><code>habp timer interval</code></td>
<td>Optional. The default interval for an HABP server to send HABP request packets is 20 seconds.</td>
</tr>
</tbody>
</table>

Table 375 Configure an HABP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable HABP</td>
<td><code>habp enable</code></td>
<td>Optional. HABP is enabled by default. And a switch operates as an HABP client after you enable HABP for it.</td>
</tr>
</tbody>
</table>

Displaying and Maintaining HABP Configuration

After performing the above configuration, you can display and verify your HABP-related configuration by execute the `display` command in any view.

Table 376 Display HABP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display HABP configuration and status</td>
<td><code>display habp</code></td>
<td>These commands can be executed in any view.</td>
</tr>
<tr>
<td>Display the MAC address table maintained by HABP</td>
<td><code>display habp table</code></td>
<td></td>
</tr>
<tr>
<td>Display statistics on HABP packets</td>
<td><code>display habp traffic</code></td>
<td></td>
</tr>
</tbody>
</table>
System Guard Overview

Guard Against IP Attacks
System-guard operates to inspect the IP packets over 10-second intervals for the CPU for suspicious source IP addresses. Once the packets from such an IP address hit the predefined threshold, System Guard does one of the following:

- The switch logs out the host (hereafter referred to as infected host) by automatically applying an ACL rule and waits a certain period of time before resuming forwarding packets for that host.
- If the packets from the infected host need processing by the CPU, the switch decreases the precedence of such packets and discards the packets already delivered to the CPU.

Guard Against TCN Attacks
System Guard monitors the rate at which TCN/TC packets are received on the ports. If a port receives an excessive number of TCN/TC packets within a given period of time, the switch sends only one TCN/TC packet in every 10 seconds to the CPU and discards the rest TCN/TC packets, while outputting trap and log information.

Layer 3 Error Control
With the Layer 3 error control feature enabled, the switch delivers all Layer 3 packets that the switch considers to be error packets to the CPU.

Configuring System Guard

Configuring System Guard Against IP Attacks
Configuration of System Guard against IP attacks includes these tasks:

- Enabling System Guard against IP attacks
- Setting the maximum number of infected hosts that can be concurrently monitored
- Configuring parameters related to MAC address learning

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable System Guard against IP</td>
<td>system-guard ip</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>enable</td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>
CHAPTER 43: SYSTEM GUARD CONFIGURATION

The correlations among the arguments of the `system-guard ip detect-threshold` command can be clearly described with this example: If you set `ip-record-threshold`, `record-times-threshold` and `isolate-time` to 30, 1 and 3 respectively, when the system detects successively three times that over 50 IP packets (destined for an address other that an IP address of the switch) from a source IP address are received within a period of 10 seconds, the system considers that it is being attacked - the system sorts out that source IP address and waits a period of 5 times the MAC address aging time before learning the destination IP address(es) of packets from that source IP address again.

Table 377  Configure System Guard against IP attacks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the maximum number of infected hosts that can be concurrently monitored</td>
<td><code>system-guard ip detect-maxnum number</code></td>
<td>Optional 30 by default</td>
</tr>
<tr>
<td>Set the maximum number of addresses that the system can learn, the maximum number of times an address can be hit before an action is taken and the address isolation time (presented in the number of multiples of MAC address aging time)</td>
<td><code>system-guard ip detect-threshold ip-record-threshold record-times-threshold isolate-time</code></td>
<td>Optional By default, <code>ip-record-threshold</code> is 30; <code>record-times-threshold</code> is 1, and <code>isolate-time</code> is 3.</td>
</tr>
</tbody>
</table>

Configuring System Guard Against TCN Attacks

Configuration of System Guard against TCN attacks includes these tasks:

- Enabling System Guard against TCN attacks
- Setting the threshold of TCN/TC packet receiving rate

Table 378  Configure System Guard against TCN attacks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable System Guard against TCN attacks</td>
<td><code>system-guard tcn enable</code></td>
<td>Required Disabled by default</td>
</tr>
<tr>
<td>Set the threshold of TCN/TC packet receiving rate</td>
<td><code>system-guard tcn rate-threshold rate-threshold</code></td>
<td>Optional 1 pps by default</td>
</tr>
</tbody>
</table>

As the system monitoring cycle is 10 seconds, the system sends trap and log information by default if more than 10 TCN/TC packets are received within 10 seconds. If the TCN/TC packet receiving rate is lower than the set threshold within a 10-second monitoring cycle, the system will not send trap or log information in the next 10-second monitoring cycle.

Enabling Layer 3 Error Control

With the following command, you can enable the Layer 3 error control feature.

Table 379  Enable Layer 3 error control

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable Layer 3 error control</td>
<td><code>system-guard l3err enable</code></td>
<td>Required Enabled by default</td>
</tr>
</tbody>
</table>
After the previously described configuration, you can use the `display` command in any view to view the running conditions of System Guard to verify your System Guard configuration.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the monitoring result and parameter settings of System Guard against IP attacks</td>
<td><code>display system-guard ip state</code></td>
<td>The <code>display</code> command can be executed in any view</td>
</tr>
<tr>
<td>Display the information about IP packets received by the CPU of the switch</td>
<td><code>display system-guard ip-record</code></td>
<td></td>
</tr>
<tr>
<td>Display the status of Layer 3 error control</td>
<td><code>display system-guard l3err state</code></td>
<td></td>
</tr>
<tr>
<td>Display the status of TCN System Guard</td>
<td><code>display system-guard tcn state</code></td>
<td></td>
</tr>
</tbody>
</table>
AAA OVERVIEW

Introduction to AAA

AAA is the acronym for the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure these three functions to implement network security management.

- Authentication: Defines what users can access the network,
- Authorization: Defines what services can be available to the users who can access the network, and
- Accounting: Defines how to charge the users who are using network resources.

Typically, AAA operates in the client/server model: the client runs on the managed resources side while the server stores the user information. Thus, AAA is well scalable and can easily implement centralized management of user information.

Authentication

AAA supports the following authentication methods:

- None authentication: Users are trusted and are not checked for their validity. Generally, this method is not recommended.
- Local authentication: User information (including user name, password, and some other attributes) is configured on this device, and users are authenticated on this device instead of on a remote device. Local authentication is fast and requires lower operational cost, but has the deficiency that information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through RADIUS or HWTACACS protocol. This device (for example, a 3Com series switch) acts as the client to communicate with the RADIUS or TACACS server. You can use standard or extended RADIUS protocols in conjunction with such systems as iTELLIN/CAMS for user authentication. Remote authentication allows convenient centralized management and is feature-rich. However, to implement remote authentication, a server is needed and must be configured properly.

Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.
- Local authorization: Users are authorized according to the related attributes configured for their local accounts on this device.
- RADIUS authorization: Users are authorized after they pass RADIUS authentication. In RADIUS protocol, authentication and authorization are combined together, and authorization cannot be performed alone without authentication.
- HWTACACS authorization: Users are authorized by a TACACS server.

**Accounting**

AAA supports the following accounting methods:
- None accounting: No accounting is performed for users.
- Remote accounting: User accounting is performed on a remote RADIUS or TACACS server.

**Introduction to ISP Domain**

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of userid@isp-name, the isp-name following the @ character is the ISP domain name. The access device uses userid as the user name for authentication, and isp-name as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different forms of user name and password, different service types/access rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

---

**Introduction to AAA Services**

**Introduction to RADIUS**

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used service for AAA is RADIUS.

**What is RADIUS**

Remote Authentication Dial-in User Service (RADIUS) is a distributed service based on client/server structure. It can prevent unauthorized access to your network and is commonly used in network environments where both high security and remote user access service are required.

The RADIUS service involves three components:
- Protocol: Based on the UDP/IP layer, RFC 2865 and 2866 define the message format and message transfer mechanism of RADIUS, and define 1812 as the authentication port and 1813 as the accounting port.
- Server: RADIUS Server runs on a computer or workstation at the center. It stores and maintains user authentication information and network service access information.
- Client: RADIUS Client runs on network access servers throughout the network.

RADIUS operates in the client/server model.

- A switch acting as a RADIUS client passes user information to a specified RADIUS server, and takes appropriate action (such as establishing/terminating user connection) depending on the responses returned from the server.
- The RADIUS server receives user connection requests, authenticates users, and returns all required information to the switch.
Generally, a RADIUS server maintains the following three databases (see Figure 149):

- **Users**: This database stores information about users (such as user name, password, protocol adopted and IP address).
- **Clients**: This database stores information about RADIUS clients (such as shared key).
- **Dictionary**: The information stored in this database is used to interpret the attributes and attribute values in the RADIUS protocol.

**Figure 149** Databases in a RADIUS server

In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

**Basic message exchange procedure in RADIUS**

The messages exchanged between a RADIUS client (a switch, for example) and a RADIUS server are verified through a shared key. This enhances the security. The RADIUS protocol combines the authentication and authorization processes together by sending authorization information along with the authentication response message. Figure 150 depicts the message exchange procedure between user, switch and RADIUS server.

**Figure 150** Basic message exchange procedure of RADIUS
The basic message exchange procedure of RADIUS is as follows:

1. The user enters the user name and password.
2. The RADIUS client receives the user name and password, and then sends an authentication request (Access-Request) to the RADIUS server.
3. The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the RADIUS client an authentication response (Access-Accept), which contains the user's authorization information. If the authentication fails, the server returns an Access-Reject response.
4. The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type attribute value = start) to the RADIUS server.
5. The RADIUS server returns a start-accounting response (Accounting-Response).
6. The user starts to access network resources.
7. The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
8. The RADIUS server returns a stop-accounting response (Accounting-Response).
9. The access to network resources is ended.

**RADIUS message format**

RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages between RADIUS server and client. As a remedy, RADIUS adopts the following mechanisms: timer management, retransmission, and backup server. Figure 151 depicts the format of RADIUS messages.
The Code field (one byte) decides the type of RADIUS message, as shown in Table 381.

**Table 381** Description of the major values of the Code field

<table>
<thead>
<tr>
<th>Code</th>
<th>Message type</th>
<th>Message description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access-Request</td>
<td>Direction: client-&gt;server. The client transmits this message to the server to determine if the user can access the network. This message carries user information. It must contain the User-Name attribute and may contain the following attributes: NAS-IP-Address, User-Password and NAS-Port.</td>
</tr>
<tr>
<td>2</td>
<td>Access-Accept</td>
<td>Direction: server-&gt;client. The server transmits this message to the client if all the attribute values carried in the Access-Request message are acceptable (that is, the user passes the authentication).</td>
</tr>
<tr>
<td>3</td>
<td>Access-Reject</td>
<td>Direction: server-&gt;client. The server transmits this message to the client if any attribute value carried in the Access-Request message is unacceptable (that is, the user fails the authentication).</td>
</tr>
<tr>
<td>4</td>
<td>Accounting-Request</td>
<td>Direction: client-&gt;server. The client transmits this message to the server to request the server to start or end the accounting (whether to start or to end the accounting is determined by the Acct-Status-Type attribute in the message). This message carries almost the same attributes as those carried in the Access-Request message.</td>
</tr>
<tr>
<td>5</td>
<td>Accounting-Response</td>
<td>Direction: server-&gt;client. The server transmits this message to the client to notify the client that it has received the Accounting-Request message and has correctly recorded the accounting information.</td>
</tr>
</tbody>
</table>

The Identifier field (one byte) is used to match requests and responses. It changes whenever the content of the Attributes field changes, and whenever a valid response has been received for a previous request, but remains unchanged for message retransmission.
3 The Length field (two bytes) specifies the total length of the message (including the Code, Identifier, Length, Authenticator and Attributes fields). The bytes beyond the length are regarded as padding and are ignored upon reception. If a received message is shorter than what the Length field indicates, it is discarded.

4 The Authenticator field (16 bytes) is used to authenticate the response from the RADIUS server; and is used in the password hiding algorithm. There are two kinds of authenticators: Request Authenticator and Response Authenticator.

5 The Attributes field contains specific authentication/authorization/accounting information to provide the configuration details of a request or response message. This field contains a list of field triplet (Type, Length and Value):

- The Type field (one byte) specifies the type of an attribute. Its value ranges from 1 to 255. Table 382 lists the attributes that are commonly used in RADIUS authentication/authorization.
- The Length field (one byte) specifies the total length of the attribute in bytes (including the Type, Length and Value fields).
- The Value field (up to 253 bytes) contains the information of the attribute. Its format is determined by the Type and Length fields.

<table>
<thead>
<tr>
<th>Type field value</th>
<th>Attribute type</th>
<th>Type field value</th>
<th>Attribute type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>23</td>
<td>Framed-IPX-Network</td>
</tr>
<tr>
<td>2</td>
<td>User-Password</td>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>3</td>
<td>CHAP-Password</td>
<td>25</td>
<td>Class</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
<td>26</td>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>27</td>
<td>Session-Timeout</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>28</td>
<td>Idle-Timeout</td>
</tr>
<tr>
<td>7</td>
<td>Framed-Protocol</td>
<td>29</td>
<td>Termination-Action</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
<td>30</td>
<td>Called-Station-Id</td>
</tr>
<tr>
<td>9</td>
<td>Framed-IP-Netmask</td>
<td>31</td>
<td>Calling-Station-Id</td>
</tr>
<tr>
<td>10</td>
<td>Framed-Routing</td>
<td>32</td>
<td>NAS-Identifier</td>
</tr>
<tr>
<td>11</td>
<td>Filter-ID</td>
<td>33</td>
<td>Proxy-State</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
<td>34</td>
<td>Login-LAT-Service</td>
</tr>
<tr>
<td>13</td>
<td>Framed-Compression</td>
<td>35</td>
<td>Login-LAT-Node</td>
</tr>
<tr>
<td>14</td>
<td>Login-IP-Host</td>
<td>36</td>
<td>Login-LAT-Group</td>
</tr>
<tr>
<td>15</td>
<td>Login-Service</td>
<td>37</td>
<td>Framed-AppleTalk-Link</td>
</tr>
<tr>
<td>16</td>
<td>Login-TCP-Port</td>
<td>38</td>
<td>Framed-AppleTalk-Network</td>
</tr>
<tr>
<td>17</td>
<td>(unassigned)</td>
<td>39</td>
<td>Framed-AppleTalk-Zone</td>
</tr>
<tr>
<td>18</td>
<td>Reply-Message</td>
<td>40-59</td>
<td>(reserved for accounting)</td>
</tr>
<tr>
<td>19</td>
<td>Callback-Number</td>
<td>60</td>
<td>CHAP-Challenge</td>
</tr>
<tr>
<td>20</td>
<td>Callback-ID</td>
<td>61</td>
<td>NAS-Port-Type</td>
</tr>
<tr>
<td>21</td>
<td>(unassigned)</td>
<td>62</td>
<td>Port-Limit</td>
</tr>
<tr>
<td>22</td>
<td>Framed-Route</td>
<td>63</td>
<td>Login-LAT-Port</td>
</tr>
</tbody>
</table>

The RADIUS protocol has good scalability. Attribute 26 (Vendor-Specific) defined in this protocol allows a device vendor to extend RADIUS to implement functions that are not defined in standard RADIUS.
Figure 152 depicts the format of attribute 26. The Vendor-ID field used to identify a vendor occupies four bytes, where the first byte is 0, and the other three bytes are defined in RFC 1700. Here, the vendor can encapsulate multiple customized sub-attributes (containing vendor-specific Type, Length and Value) to implement a RADIUS extension.

**Figure 152**  Vendor-specific attribute format

<table>
<thead>
<tr>
<th></th>
<th>Type</th>
<th>Length</th>
<th>Vendor-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>15</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**What is HWTACACS**

3Com Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP, VPDN, and terminal users) through communicating with TACACS server in client-server mode.

Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. Table 383 lists the primary differences between HWTACACS and RADIUS.

**Table 383**  Differences between HWTACACS and RADIUS

<table>
<thead>
<tr>
<th>HWTACACS</th>
<th>RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adopts TCP, providing more reliable network transmission.</td>
<td>Adopts UDP.</td>
</tr>
<tr>
<td>Encrypts the entire message except the HWTACACS header.</td>
<td>Encrypts only the password field in authentication message.</td>
</tr>
<tr>
<td>Separates authentication from authorization. For example, you can use one TACACS server for authentication and another TACACS server for authorization.</td>
<td>Combines authentication and authorization.</td>
</tr>
<tr>
<td>Is more suitable for security control.</td>
<td>Is more suitable for accounting.</td>
</tr>
<tr>
<td>Supports configuration command authorization.</td>
<td>Does not support.</td>
</tr>
</tbody>
</table>

In a typical HWTACACS application (as shown in Figure 153), a terminal user needs to log into the switch to perform some operations. As a HWTACACS client, the switch sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user successfully logs into the switch to perform operations.
Basic message exchange procedure in HWTACACS

The following text takes telnet user as an example to describe how HWTACACS implements authentication, authorization, and accounting for a user. Figure 154 illustrates the basic message exchange procedure:

Figure 154  AAA implementation procedure for a telnet user
The basic message exchange procedure is as follows:

1. A user sends a login request to the switch acting as a TACACS client, which then sends an authentication start request to the TACACS server.
2. The TACACS server returns an authentication response, asking for the username. Upon receiving the response, the TACACS client requests the user for the username.
3. After receiving the username from the user, the TACACS client sends an authentication continuance message carrying the username.
4. The TACACS server returns an authentication response, asking for the password. Upon receiving the response, the TACACS client requests the user for the login password.
5. After receiving the password, the TACACS client sends an authentication continuance message carrying the password to the TACACS server.
6. The TACACS server returns an authentication response, indicating that the user has passed the authentication.
7. The TACACS client sends a user authorization request to the TACACS server.
8. The TACACS server returns an authorization response, indicating that the user has passed the authorization.
9. After receiving the response indicating an authorization success, the TACACS client pushes the configuration interface of the switch to the user.
10. The TACACS client sends an accounting start request to the TACACS server.
11. The TACACS server returns an accounting response, indicating that it has received the accounting start request.
12. The user logs out; the TACACS client sends an accounting stop request to the TACACS server.
13. The TACACS server returns an accounting response, indicating that it has received the accounting stop request.
AAA Configuration

Task List

You need to configure AAA to provide network access services for legal users while protecting network devices and preventing unauthorized access and repudiation behavior.

Table 384  AAA configuration tasks (configuring a combined AAA scheme for an ISP domain)

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA configuration</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating an ISP Domain and Configuring Its Attributes”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring a combined AAA scheme”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring an AAA Scheme for an ISP Domain”</td>
<td>Use one of the authentication methods</td>
</tr>
<tr>
<td>None authentication</td>
<td>Use one of the authentication methods</td>
</tr>
<tr>
<td>Local authentication</td>
<td>You need to configure RADIUS or HWATACACS before performing RADIUS or HWATACACS authentication</td>
</tr>
<tr>
<td>RADIUS authentication</td>
<td></td>
</tr>
<tr>
<td>HWTACACS authentication</td>
<td></td>
</tr>
<tr>
<td>“Configuring Dynamic VLAN Assignment”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Attributes of a Local User”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Cutting Down User Connections Forcibly”</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Table 385  AAA configuration tasks (configuring separate AAA schemes for an ISP domain)

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| AAA configuration
  “Creating an ISP Domain and Configuring Its Attributes” | Required |
| “Configuring separate AAA schemes” | Required |
| “Configuring an AAA Scheme for an ISP Domain” | Required |

- With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively.
- You need to configure RADIUS or HWATACACS before performing RADIUS or HWTACACS authentication.

“Configuring Dynamic VLAN Assignment” | Optional |
“Configuring the Attributes of a Local User” | Optional |
“Cutting Down User Connections Forcibly” | Optional |

Table 386  Create an ISP domain and configure its attributes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create an ISP domain or set an ISP domain as the default ISP domain</td>
<td>domain { isp-name</td>
<td>default { disable</td>
</tr>
<tr>
<td>If no ISP domain is set as the default ISP domain, the ISP domain system is used as the default ISP domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the status of the ISP domain</td>
<td>state { active</td>
<td>block }</td>
</tr>
<tr>
<td>By default, an ISP domain is in the active state, that is, all the users in the domain are allowed to request network service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of access users that the ISP domain can accommodate</td>
<td>access-limit { disable</td>
<td>enable max-user-number }</td>
</tr>
<tr>
<td>By default, there is no limit on the number of access users that the ISP domain can accommodate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the idle-cut function</td>
<td>idle-cut { disable</td>
<td>enable minute flow }</td>
</tr>
<tr>
<td>By default, the idle-cut function is disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the accounting-optional switch</td>
<td>accounting optional</td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the accounting-optional switch is off.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AAA Configuration Task List

**Table 386** Create an ISP domain and configure its attributes

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the messenger function</td>
<td>messenger time { enable limit interval</td>
<td>disable }</td>
</tr>
<tr>
<td>Set the self-service server location function</td>
<td>self-service-url { disable</td>
<td>enable url-string }</td>
</tr>
</tbody>
</table>

**Note that:**

- **On the Switch 5500,** each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the switch. When a user logs in, if no ISP domain name is carried in the user name, the switch assumes that the user belongs to the default ISP domain.

- The @ character must not appear more than once in the user name.

- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for a user, it does not disconnect the user as long as the accounting optional command has been executed, though it cannot perform accounting for the user in this case.

- The self-service server location function needs the cooperation of a RADIUS server that supports self-service, such as Comprehensive Access Management Server (CAMS). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with self-service software is called a self-service server.

3Com’s CAMS Server is a service management system used to manage networks and ensure network and user information security. With the cooperation of other networking devices (such as switches) in a network, a CAMS server can implement the AAA functions and right management.

### Configuring an AAA Scheme for an ISP Domain

You can configure either a combined or a separate AAA scheme. Each is described below:

#### Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain. If you specify a RADIUS or HWTACACS scheme, the authentication, authorization and accounting will be uniformly implemented by the RADIUS or TACACS server(s) specified in the RADIUS or HWTACACS scheme. In this way, you cannot specify different schemes for authentication, authorization and accounting respectively.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create an ISP domain and enter its view, or enter the view of an existing ISP domain</td>
<td>domain isp-name</td>
<td>Required</td>
</tr>
</tbody>
</table>
CAUTION:

- You can execute the `scheme radius-scheme radius-scheme-name` command to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.

- If you execute the `scheme radius-scheme radius-scheme-name local` command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, the local scheme is not used; otherwise, the local scheme is used.

- If you execute the `scheme hwtacacs-scheme hwtacacs-scheme-name local` command, the local scheme is used as the secondary scheme in case no TACACS server is available. That is, if the communication between the switch and a TACACS server is normal, the local scheme is not used; if the TACACS server is not reachable or there is a key error or NAS IP error, the local scheme is used.

- If you execute the `scheme local` or `scheme none` command to adopt local or none as the primary scheme, the local authentication is performed or no authentication is performed. In this case you cannot specify any RADIUS scheme or HWTACACS scheme at the same time.

- If you configure none as the primary scheme, the domain’s FTP users cannot pass authentication. Therefore, you cannot specify none as the primary scheme if you want to enable FTP service.

### Configuring separate AAA schemes

You can use the `authentication`, `authorization`, and `accounting` commands to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. The following gives the implementations of this separate way for the services supported by AAA.

1. **For terminal users**
   - Authentication: RADIUS, local, HWTACACS or none.
   - Authorization: none or HWTACACS.
   - Accounting: RADIUS, HWTACACS or none.
   
   You can use an arbitrary combination of the above implementations for your AAA scheme configuration.

2. **For FTP users**
   - Only authentication is supported for FTP users.
Authentication: RADIUS, local, or HWTACACS.

**Table 388  Configure separate AAA schemes**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create an ISP domain and enter its view, or enter the view of an existing ISP domain</td>
<td>domain isp-name</td>
<td>Required</td>
</tr>
<tr>
<td>Configure an authentication scheme for the ISP domain</td>
<td>authentication { radius-scheme radius-scheme-name [ local ]</td>
<td>hwtacacs-scheme hwtacacs-scheme-name [ local ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no separate authentication scheme is configured.</td>
</tr>
<tr>
<td>Configure a HWTACACS authentication scheme for user level switching</td>
<td>authentication super hwtacacs-scheme hwtacacs-scheme-name</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no HWTACACS authentication scheme is configured.</td>
</tr>
<tr>
<td>Configure an authorization scheme for the ISP domain</td>
<td>authorization { none</td>
<td>hwtacacs-scheme hwtacacs-scheme-name }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no separate authorization scheme is configured.</td>
</tr>
<tr>
<td>Configure an accounting scheme for the ISP domain</td>
<td>accounting { none</td>
<td>radius-scheme radius-scheme-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no separate accounting scheme is configured.</td>
</tr>
</tbody>
</table>

- If a combined AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.
- RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make authentication and authorization configuration for a domain: When the `scheme radius-scheme` or `scheme local` command is executed and the `authentication` command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect even if the `authorization none` command is executed.
- The Switch 5500 adopts hierarchical protection for command lines so as to inhibit users at lower levels from using higher level commands to configure the switches. For details about configuring a HWTACACS authentication scheme for low-to-high user level switching, refer to the section entitled “User Level Switching” on page 20.

**Configuration guidelines**

Suppose a combined AAA scheme is available. The system selects AAA schemes according to the following principles:

- If authentication, authorization, accounting each have a separate scheme, the separate schemes are used.
- If you configure only a separate authentication scheme (that is, there are no separate authorization and accounting schemes configured), the combined
scheme is used for authorization and accounting. In this case, if the combined scheme uses RADIUS or HWTACACS, the system never uses the secondary scheme for authorization and accounting.

- If you configure no separate scheme, the combined scheme is used for authentication, authorization, and accounting. In this case, if the system uses the secondary local scheme for authentication, it also does so for authorization and accounting; if the system uses the first scheme for authentication, it also does so for authorization and accounting, even if authorization and accounting fail.

**Configuring Dynamic VLAN Assignment**

The dynamic VLAN assignment feature enables a switch to dynamically add the switch ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the switch supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.

- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

In actual applications, to use this feature with a Guest VLAN, you should set the port control to port-based mode. For more information, refer to “802.1x Configuration” on page 477.

<table>
<thead>
<tr>
<th>Table 389</th>
<th>Configure dynamic VLAN assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Create an ISP domain and enter its view</td>
<td>domain isp-name</td>
</tr>
<tr>
<td>Set the VLAN assignment mode</td>
<td>vlan-assignment-mode { integer</td>
</tr>
<tr>
<td>Create a VLAN and enter its view</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>Set a VLAN name for VLAN assignment</td>
<td>name string</td>
</tr>
</tbody>
</table>
CAUTION:

- In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).

- To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.

Configuring the Attributes of a Local User

When local scheme is chosen as the AAA scheme, you should create local users on the switch and configure the relevant attributes.

The local users are users set on the switch, with each user uniquely identified by a user name. To make a user who is requesting network service pass local authentication, you should add an entry in the local user database on the switch for the user.

Table 390  Configure the attributes of a local user

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set the password display mode of</td>
<td>local-user password-display-mode</td>
<td>Optional</td>
</tr>
<tr>
<td>all local users</td>
<td>{cipher-force</td>
<td>auto }</td>
</tr>
<tr>
<td>Add a local user and enter local</td>
<td>local-user user-name</td>
<td>Required</td>
</tr>
<tr>
<td>user view</td>
<td></td>
<td>By default, there is no local user in the system.</td>
</tr>
<tr>
<td>Set a password for the local user</td>
<td>password { simple</td>
<td>cipher }</td>
</tr>
<tr>
<td>Set the status of the local user</td>
<td>state { active</td>
<td>block }</td>
</tr>
<tr>
<td>Authorize the user to access</td>
<td>service-type { ftp</td>
<td>lan-access</td>
</tr>
<tr>
<td>specified type(s) of service</td>
<td></td>
<td>By default, the system does not authorize the user to access any service.</td>
</tr>
<tr>
<td>Set the privilege level of the</td>
<td>level level</td>
<td>Optional</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>By default, the privilege level of the user is 0.</td>
</tr>
<tr>
<td>Configure the authorization VLAN</td>
<td>authorization vlan string</td>
<td>Optional</td>
</tr>
<tr>
<td>for the local user</td>
<td></td>
<td>By default, no authorization VLAN is configured for the local user.</td>
</tr>
</tbody>
</table>
**CAUTION:**

- The following characters are not allowed in the user-name string: /:*?<>. And you cannot input more than one @ in the string.

- After the local-user password-display-mode cipher-force command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the password command.

- If a user name and password is required for user authentication (RADIUS authentication as well as local authentication), the command level that a user can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels set on their user interfaces.

- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.

- If the clients connected to a port have different authorization VLANs, only the first client passing the MAC address authentication can be assigned with an authorization VLAN. The switch will not assign authorization VLANs for subsequent users passing MAC address authentication. In this case, you are recommended to connect only one MAC address authentication user or multiple users with the same authorization VLAN to a port.

- For local RADIUS authentication or local authentication to take effect, the VLAN assignment mode must be set to string after you specify authorization VLANs for local users.

<table>
<thead>
<tr>
<th>Table 390</th>
<th>Configure the attributes of a local user</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Set the attributes of the user whose service type is lan-access</td>
<td>attribute { ip ip-address</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 391</th>
<th>Cut down user connections forcibly</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
</tbody>
</table>
You can use the `display connection` command to view the connections of Telnet users, but you cannot use the `cut connection` command to cut down their connections.

### RADIUS Configuration Task List

3Com’s Ethernet switches can function not only as RADIUS clients but also as local RADIUS servers.

#### Table 391  Cut down user connections forcibly

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut down user connections forcibly</td>
<td>`cut connection { all</td>
<td>access-type { dot1x</td>
</tr>
</tbody>
</table>

### Table 392  RADIUS configuration tasks (the switch functions as a RADIUS client)

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the RADIUS client</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating a RADIUS Scheme”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring RADIUS Authentication/Authorization Servers”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring RADIUS Accounting Servers”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring Shared Keys for RADIUS Messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Maximum Number of RADIUS Request Transmission Attempts”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Type of RADIUS Servers to be Supported”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Status of RADIUS Servers”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Attributes of Data to be Sent to RADIUS Servers”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring Timers for RADIUS Servers”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Enabling Sending Trap Message when a RADIUS Server Goes Down”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Enabling the User Re-Authentication at Restart Function”</td>
<td>Optional</td>
</tr>
</tbody>
</table>
The RADIUS service configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each type of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has some parameters such as IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.

<table>
<thead>
<tr>
<th>Table 392</th>
<th>RADIUS configuration tasks (the switch functions as a RADIUS client)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Remarks</td>
</tr>
<tr>
<td>Configuring the RADIUS server</td>
<td>Refer to “Creating a RADIUS Scheme” on page 532. Required</td>
</tr>
<tr>
<td>Configuring RADIUS Authentication/Authorization Servers</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring RADIUS Accounting Servers</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring Shared Keys for RADIUS Messages</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Maximum Number of RADIUS Request Transmission Attempts</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Type of RADIUS Servers to be Supported</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Status of RADIUS Servers</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Attributes of Data to be Sent to RADIUS Servers</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Local RADIUS Authentication Server</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring Timers for RADIUS Servers</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling Sending Trap Message when a RADIUS Server Goes Down</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the RADIUS client</td>
<td>Refer to “Configuring the Type of RADIUS Servers to be Supported” on page 532</td>
</tr>
</tbody>
</table>

The RADIUS service configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each type of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has some parameters such as IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.
In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server, and you should keep the RADIUS server port settings on the switch consistent with those on the RADIUS servers.

Actually, the RADIUS service configuration only defines the parameters for information exchange between switch and RADIUS server. To make these parameters take effect, you must reference the RADIUS scheme configured with these parameters in an ISP domain view (refer to “AAA Configuration Task List” on page 519).

Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

**Table 394** Create a RADIUS scheme

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable RADIUS authentication port</td>
<td>radius client enable</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, RADIUS authentication port is enabled.</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a RADIUS scheme named system has already been created in the system.</td>
</tr>
</tbody>
</table>

A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

Configuring RADIUS Authentication/Authorization Servers

**Table 395** Configure RADIUS authentication/authorization servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>Required</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a RADIUS scheme named system has already been created in the system.</td>
</tr>
<tr>
<td>Set the IP address and port number of the primary RADIUS authentication/authorization server</td>
<td>primary authentication ip-address [ port-number ]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.</td>
</tr>
<tr>
<td>Set the IP address and port number of the secondary RADIUS authentication/authorization server</td>
<td>secondary authentication ip-address [ port-number ]</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.</td>
</tr>
</tbody>
</table>
The authentication response sent from the RADIUS server to the RADIUS client carries authorization information. Therefore, you need not (and cannot) specify a separate RADIUS authorization server.

In an actual network environment, you can specify one server as both the primary and secondary authentication/authorization servers, as well as specifying two RADIUS servers as the primary and secondary authentication/authorization servers respectively.

The IP address and port number of the primary authentication server used by the default RADIUS scheme system are 127.0.0.1 and 1645.

---

### Configuring RADIUS Accounting Servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td>Set the IP address and port number of the primary RADIUS accounting server</td>
<td>primary accounting ip-address [ port-number ]</td>
<td>Required</td>
</tr>
<tr>
<td>Set the IP address and port number of the secondary RADIUS accounting server</td>
<td>secondary accounting ip-address [ port-number ]</td>
<td>Optional</td>
</tr>
<tr>
<td>Enable stop-accounting request buffering</td>
<td>stop-accounting-buffer enable</td>
<td>Optional</td>
</tr>
<tr>
<td>Set the maximum number of transmission attempts of a buffered stop-accounting request.</td>
<td>retry stop-accounting retry-times</td>
<td>Optional</td>
</tr>
<tr>
<td>Set the maximum allowed number of continuous real-time accounting failures</td>
<td>retry realtime-accounting retry-times</td>
<td>Optional</td>
</tr>
</tbody>
</table>

In an actual network environment, you can specify one server as both the primary and secondary accounting servers, as well as specifying two RADIUS servers as the primary and secondary accounting servers respectively. In addition, because RADIUS adopts different UDP ports to exchange authentication/authorization messages and accounting messages, you must set
a port number for accounting different from that set for authentication/authorization.

- With stop-accounting request buffering enabled, the switch first buffers the stop-accounting request that gets no response from the RADIUS accounting server, and then retransmits the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

- You can set the maximum allowed number of continuous real-time accounting failures. If the number of continuously failed real-time accounting requests to the RADIUS server reaches the set maximum number, the switch cuts down the user connection.

- The IP address and port number of the primary accounting server of the default RADIUS scheme system are 127.0.0.1 and 1646 respectively.

- Currently, RADIUS does not support the accounting of FTP users.

Configuring Shared Keys for RADIUS Messages

Both RADIUS client and server adopt MD5 algorithm to encrypt RADIUS messages before they are exchanged between the two parties. The two parties verify the validity of the RADIUS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Table 397 Configure shared keys for RADIUS messages

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>radius-scheme-name</td>
<td>By default, a RADIUS scheme named system has already been created in the system.</td>
</tr>
<tr>
<td>Set a shared key for RADIUS authentication/authorization messages</td>
<td>key authentication string</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no shared key is created.</td>
</tr>
<tr>
<td>Set a shared key for RADIUS accounting messages</td>
<td>key accounting string</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no shared key is created.</td>
</tr>
</tbody>
</table>

**CAUTION:** The authentication/authorization shared key and the accounting shared key you set on the switch must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

Configuring the Maximum Number of RADIUS Request Transmission Attempts

The communication in RADIUS is unreliable because this protocol uses UDP packets to carry its data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the switch gets no answer after it has tried the maximum number of times to transmit the request, the switch considers that the request fails.
Configuring the Type of RADIUS Servers to be Supported

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td>Set the maximum number of RADIUS request transmission attempts</td>
<td>retry retry-times</td>
<td>Optional</td>
</tr>
</tbody>
</table>

If you change the RADIUS server type, the units of data flows sent to RADIUS servers will be restored to the defaults.

When the third party RADIUS server is used, you can select standard or extended as the server-type in a RADIUS scheme; when the CAMS server is used, you can select extended as the server-type in a RADIUS scheme.

Configuring the Status of RADIUS Servers

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the block state for a set time (set by the timer quiet command), the switch will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to active while keeping the status of the secondary server unchanged.

When both the primary and secondary servers are in active or block state, the switch sends messages only to the primary server.
RADIUS Configuration Task List

Table 400  Set the status of RADIUS servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td>Set the status of the primary RADIUS authentication/authorization server</td>
<td>state primary authentication { block</td>
<td>active }</td>
</tr>
<tr>
<td>Set the status of the primary RADIUS accounting server</td>
<td>state primary accounting { block</td>
<td>active }</td>
</tr>
<tr>
<td>Set the status of the secondary RADIUS authentication/authorization server</td>
<td>state secondary authentication { block</td>
<td>active }</td>
</tr>
<tr>
<td>Set the status of the secondary RADIUS accounting server</td>
<td>state secondary accounting { block</td>
<td>active }</td>
</tr>
</tbody>
</table>

Table 401  Configure the attributes of data to be sent to RADIUS servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td>radius scheme radius-scheme-name</td>
<td>Required</td>
</tr>
<tr>
<td>Set the format of the user names to be sent to RADIUS server</td>
<td>user-name-format { with-domain</td>
<td>without-domain }</td>
</tr>
<tr>
<td>Set the units of data flows to RADIUS servers</td>
<td>data-flow-format data { byte</td>
<td>giga-byte</td>
</tr>
<tr>
<td>Set the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets</td>
<td>calling-station-id mode { mode1</td>
<td>mode2 } { lowercase</td>
</tr>
<tr>
<td>Set the source IP address of outgoing RADIUS messages</td>
<td>RADIUS scheme view nas-ip ip-address System view radius nas-ip ip-address</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Generally, the access users are named in the userid@isp-name format. Here, isp-name after the @ character represents the ISP domain name, by which the
device determines which ISP domain a user belongs to. However, some old RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove domain names from user names before sending the user names to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the user names to be sent to RADIUS server.

- For a RADIUS scheme, if you have specified to remove ISP domain names from user names, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).

- In the default RADIUS scheme **system**, ISP domain names are removed from user names by default.

- The purpose of setting the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets is to improve the switch’s compatibility with different RADIUS servers. This setting is necessary when the format of Calling-Station-Id field recognizable to RADIUS servers is different from the default MAC address format on the switch. For details about field formats recognizable to RADIUS servers, refer to the corresponding RADIUS server manual.

---

**Configuring the Local RADIUS Authentication Server Function**

The switch provides the local RADIUS server function (including authentication and authorization), also known as the local RADIUS authentication server function, in addition to RADIUS client service, where separate authentication/authorization server and the accounting server are used for user authentication.

**Table 402  Configure the local RADIUS authentication server function**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><em>system-view</em></td>
<td>-</td>
</tr>
<tr>
<td>Enable UDP port for local</td>
<td><em>local-server enable</em></td>
<td>Optional</td>
</tr>
<tr>
<td>RADIUS authentication server</td>
<td></td>
<td>By default, the UDP port for local RADIUS authentication server is enabled.</td>
</tr>
<tr>
<td>Configure the parameters of</td>
<td><em>local-server nas-ip</em></td>
<td>Required</td>
</tr>
<tr>
<td>the local RADIUS server</td>
<td><em>ip-address</em>  <em>key</em>  <em>password</em></td>
<td>By default, a local RADIUS authentication server is configured with an NAS IP address of 127.0.0.1.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- If you adopt the local RADIUS authentication server function, the UDP port number of the authentication/authorization server must be 1645, the UDP port number of the accounting server must be 1646, and the IP addresses of the servers must be set to the addresses of this switch.

- The message encryption key set by the **local-server nas-ip ip-address key password** command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this switch as its authentication server.
The switch supports IP addresses and shared keys for up to 16 network access servers (NAS). That is, when acting as the local RADIUS authentication server, the switch can provide authentication service to up to 16 network access servers (including the switch itself) at the same time.

When acting as the local RADIUS authentication server, the switch does not support EAP authentication.

### Configuring Timers for RADIUS Servers

After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the switch waits for a response from the server. The maximum time that the switch can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the switch system is called the response timeout timer of RADIUS servers. If the switch gets no answer within the response timeout time, it needs to retransmit the request to ensure that the user can obtain RADIUS service.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the **block** state for a specific time (set by the `timer quiet` command), the switch will try to communicate with the primary server again when it has a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to **active** while keeping the status of the secondary server unchanged.

To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users’ accounting information to RADIUS server at the set interval.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Create a RADIUS scheme and enter its view</td>
<td><code>radius scheme</code> <code>radius-scheme-name</code></td>
<td>Required</td>
</tr>
<tr>
<td>By default, a RADIUS scheme named <strong>system</strong> has already been created in the system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the response timeout time of RADIUS servers</td>
<td><code>timer response-timeout</code> <code>seconds</code></td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the response timeout time of RADIUS servers is three seconds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the time that the switch waits before it try to re-communicate with primary server and restore the status of the primary server to active</td>
<td><code>timer quiet</code> <code>minutes</code></td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the switch waits five minutes before it restores the status of the primary server to active.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 45: AAA CONFIGURATION

Enabling Sending Trap Message when a RADIUS Server Goes Down

- This configuration takes effect on all RADIUS schemes.
- The switch considers a RADIUS server as being down if it has tried the configured maximum times to send a message to the RADIUS server but does not receive any response.

Table 403 Set timers for RADIUS servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the real-time accounting interval</td>
<td>timer realtime-accounting</td>
<td>Optional by default, the real-time accounting interval is 12 minutes.</td>
</tr>
<tr>
<td></td>
<td>minutes</td>
<td></td>
</tr>
</tbody>
</table>

Table 404 Specify to send trap message when a RADIUS server goes down

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the sending of trap message when a RADIUS server is down</td>
<td>radius trap { authentication-server-down</td>
<td>Optional by default, the switch does not send trap message when a RADIUS server is down.</td>
</tr>
<tr>
<td></td>
<td>accounting-server-down }</td>
<td></td>
</tr>
</tbody>
</table>

Enabling the User Re-Authentication at Restart Function

The user re-authentication at restart function applies only to the environment where the RADIUS authentication/authorization and accounting server is CAMS.

In an environment that a CAMS server is used to implement AAA functions, if the switch reboots after an exclusive user (a user whose concurrent online number is set to 1 on the CAMS) gets authenticated and authorized and begins being charged, the switch will give a prompt that the user has already been online when the user re-logs into the network before the CAMS performs online user detection, and the user cannot get authenticated. In this case, the user can access the network again only when the CAMS administrator manually removes the user’s online information.

The user re-authentication at restart function is designed to resolve this problem. After this function is enabled, every time the switch restarts:

1. The switch generates an Accounting-On message, which mainly contains the following information: NAS-ID, NAS-IP-address (source IP address), and session ID.
2. The switch sends the Accounting-On message to the CAMS at regular intervals.
3. Once the CAMS receives the Accounting-On message, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who were accessing the network through the switch before the restart according to the information (NAS-ID, NAS-IP-address and session ID) contained in the message, and ends the accounting for the users depending on the last accounting update message.
4 Once the switch receives the response from the CAMS, it stops sending Accounting-On messages.

5 If the switch does not receive any response from the CAMS after it has tried the configured maximum number of times to send the Accounting-On message, it will not send the Accounting-On message any more.

The switch can automatically generate the main attributes (NAS-ID, NAS-IP-address and session ID) contained in Accounting-On messages. However, you can also manually configure the NAS-IP-address with the `nas-ip` command. If you choose to manually configure the attribute, be sure to configure an appropriate valid IP address. If this attribute is not configured, the switch will automatically choose the IP address of a VLAN interface as the NAS-IP-address.

Table 405 Enable the user re-authentication at restart function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter RADIUS scheme view</td>
<td>radius scheme</td>
<td></td>
</tr>
<tr>
<td></td>
<td>radius-scheme-name</td>
<td></td>
</tr>
<tr>
<td>Enable the user re-authentication at restart function</td>
<td>accounting-on enable [send times</td>
<td>By default, this function is disabled. If you use this command without any parameter, the system will try at most 15 times to send an Accounting-On message at the interval of three seconds.</td>
</tr>
<tr>
<td></td>
<td>interval ]</td>
<td></td>
</tr>
</tbody>
</table>

Table 406 HWTACACS configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the TACACS client</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating a HWTACACS Scheme” on page 538</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating a HWTACACS Scheme” on page 538</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating a HWTACACS Scheme” on page 538</td>
<td>Required</td>
</tr>
<tr>
<td>“Creating Shared Keys for RADIUS Messages” on page 531</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Attributes of Data to be Sent to TACACS Servers” on page 540</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Timers Regarding TACACS Servers” on page 541</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the TACACS server</td>
<td>Refer to “Configuring TACACS Accounting Servers” on page 539</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>
Creating a HWTACACS Scheme

The HWTACACS protocol configuration is performed on a scheme basis. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before performing other configuration tasks.

Table 407  Create a HWTACACS scheme

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
<td>Required By default, no HWTACACS scheme exists.</td>
</tr>
</tbody>
</table>

**CAUTION:**
- The system supports up to 16 HWTACACS schemes. You can delete a HWTACACS scheme only when it is not referenced.
- If the Fabric function is enabled on the switch, you cannot create any HWTACACS scheme, because the two are exclusive to each other.

Configuring TACACS Authentication Servers

Table 408  Configure TACACS authentication servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
<td>Required By default, no HWTACACS scheme exists.</td>
</tr>
<tr>
<td>Set the IP address and port number of the primary TACACS authentication server</td>
<td>primary authentication ip-address [ port ]</td>
<td>Required By default, the IP address of the primary authentication server is 0.0.0.0, and the port number is 0.</td>
</tr>
<tr>
<td>Set the IP address and port number of the secondary TACACS authentication server</td>
<td>secondary authentication ip-address [ port ]</td>
<td>Optional By default, the IP address of the secondary authentication server is 0.0.0.0, and the port number is 0.</td>
</tr>
</tbody>
</table>

**CAUTION:**
- You are not allowed to configure the same IP address for both primary and secondary authentication servers. If you do this, the system will prompt that the configuration fails.
- You can remove an authentication server setting only when there is no active TCP connection that is sending authentication messages to the server.

Configuring TACACS Authorization Servers

Table 409  Configure TACACS authorization servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 409  Configure TACACS authorization servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td><code>hwtacacs scheme</code> <code>hwtacacs-scheme-name</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no HWTACACS scheme exists.</td>
</tr>
<tr>
<td>Set the IP address and port number of the primary TACACS authorization server</td>
<td><code>primary authorization</code> <code>ip-address [ port ]</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address of the primary authorization server is 0.0.0.0, and the port number is 0.</td>
</tr>
<tr>
<td>Set the IP address and port number of the secondary TACACS authorization server</td>
<td><code>secondary authorization</code> <code>ip-address [ port ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address of the secondary authorization server is 0.0.0.0, and the port number is 0.</td>
</tr>
</tbody>
</table>

**CAUTION:**
- You are not allowed to configure the same IP address for both primary and secondary authorization servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending authorization messages.

Configure TACACS Accounting Servers

Table 410  Configure TACACS accounting servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td><code>hwtacacs scheme</code> <code>hwtacacs-scheme-name</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no HWTACACS scheme exists.</td>
</tr>
<tr>
<td>Set the IP address and port number of the primary TACACS accounting server</td>
<td><code>primary accounting</code> <code>ip-address [ port ]</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address of the primary accounting server is 0.0.0.0, and the port number is 0.</td>
</tr>
<tr>
<td>Set the IP address and port number of the secondary TACACS accounting server</td>
<td><code>secondary accounting</code> <code>ip-address [ port ]</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the IP address of the secondary accounting server is 0.0.0.0, and the port number is 0.</td>
</tr>
<tr>
<td>Enable the stop-accounting message retransmission function and set the maximum number of transmission attempts of a buffered stop-accounting message</td>
<td><code>retry stop-accounting</code> <code>retry-times</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the stop-accounting messages retransmission function is enabled and the system can transmit a buffered stop-accounting request for 100 times.</td>
</tr>
</tbody>
</table>

**CAUTION:**
CHAPTER 45: AAA CONFIGURATION

- You are not allowed to configure the same IP address for both primary and secondary accounting servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending accounting messages.

Configuring Shared Keys for HWTACACS Messages

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the switch and the TACACS server.

The TACACS client and server adopt MD5 algorithm to encrypt HWTACACS messages before they are exchanged between the two parties. The two parties verify the validity of the HWTACACS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

<table>
<thead>
<tr>
<th>Table 411</th>
<th>Configure shared keys for HWTACACS messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
<tr>
<td>Set a shared key for HWTACACS authentication, authorization or accounting messages</td>
<td>key (accounting</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>authorization</td>
</tr>
<tr>
<td></td>
<td>authentication</td>
</tr>
</tbody>
</table>

Configuring the Attributes of Data to be Sent to TACACS Servers

<table>
<thead>
<tr>
<th>Table 412</th>
<th>Configure the attributes for data to be sent to TACACS servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
<tr>
<td>Set the format of the user names to be sent to TACACS server</td>
<td>user-name-format { with-domain</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>without-domain }</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the units of data flows to TACACS servers</td>
<td>data-flow-format data { byte</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>data-flow-format packet { giga-packet</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the source IP address of outgoing HWTACACS messages</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System view</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hwtacacs nas-ip ip-address</td>
</tr>
</tbody>
</table>
CAUTION: Generally, the access users are named in the userid@isp-name format. Where, isp-name after the @ character represents the ISP domain name. If the TACACS server does not accept the user names that carry ISP domain names, it is necessary to remove domain names from user names before they are sent to TACACS server.

Configuring the Timers Regarding TACACS Servers

Table 413 Configure the timers regarding TACACS servers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a HWTACACS scheme and enter its view</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
<td>Required By default, no HWTACACS scheme exists.</td>
</tr>
<tr>
<td>Set the response timeout time of TACACS servers</td>
<td>timer response-timeout seconds</td>
<td>Optional By default, the response timeout time is five seconds.</td>
</tr>
<tr>
<td>Set the time that the switch must wait before it can restore the status of the primary server to active</td>
<td>timer quiet minutes</td>
<td>Optional By default, the switch must wait five minutes before it can restore the status of the primary server to active.</td>
</tr>
<tr>
<td>Set the real-time accounting interval</td>
<td>timer realtime-accounting minutes</td>
<td>Optional By default, the real-time accounting interval is 12 minutes.</td>
</tr>
</tbody>
</table>

CAUTION:
- To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users’ accounting information to the TACACS server at the set interval.
- The real-time accounting interval must be a multiple of 3.
- The setting of real-time accounting interval somewhat depends on the performance of the TACACS client and server devices: A shorter interval requires higher device performance.

Displaying and Maintaining AAA Configuration

After completing the above configuration, you can execute the display commands in any view to view the configuration result and operation status of AAA, RADIUS and HWTACACS and verify your configuration.

You can use the reset command in user view to clear the corresponding statistics.
### Table 414  Display AAA information

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configuration information about one specific or all ISP domains</td>
<td>display domain [isp-name]</td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display information about user connections</td>
<td>display connection [access-type {dot1x</td>
<td>mac-authentication}</td>
</tr>
<tr>
<td>Display information about user connections</td>
<td>display local-user [domain isp-name</td>
<td>idle-cut {disable</td>
</tr>
</tbody>
</table>

### Table 415  Display and maintain RADIUS protocol information

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display RADIUS message statistics about local RADIUS authentication server</td>
<td>display local-server statistics</td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display configuration information about one specific or all RADIUS schemes</td>
<td>display radius scheme [radius-scheme-name]</td>
<td></td>
</tr>
<tr>
<td>Display RADIUS message statistics</td>
<td>display radius statistics</td>
<td></td>
</tr>
<tr>
<td>Display buffered non-response stop-accounting requests</td>
<td>display stop-accounting-buffer {radius-scheme radius-scheme-name</td>
<td>session-id session-id</td>
</tr>
<tr>
<td>Delete buffered non-response stop-accounting requests</td>
<td>reset stop-accounting-buffer {radius-scheme radius-scheme-name</td>
<td>session-id session-id</td>
</tr>
<tr>
<td>Clear RADIUS message statistics</td>
<td>reset radius statistics</td>
<td></td>
</tr>
</tbody>
</table>
Remote RADIUS Authentication of Telnet/SSH Users

The configuration procedure for remote authentication of SSH users by RADIUS server is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for remote authentication.

Network requirements

In the network environment shown in Figure 155, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- A RADIUS authentication server with IP address 10.110.91.164 is connected to the switch.
- On the switch, set the shared key it uses to exchange messages with the authentication RADIUS server to aabbcc.
- A CAMS server is used as the RADIUS server. You can select extended as the server-type in a RADIUS scheme.
- On the RADIUS server, set the shared key it uses to exchange messages with the switch to aabbcc, set the authentication port number, and add Telnet user names and login passwords.

The Telnet user names added to the RADIUS server must be in the format of userid@isp-name if you have configured the switch to include domain names in the user names to be sent to the RADIUS server in the RADIUS scheme.

Table 416  Display and maintain HWTACACS protocol information

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configuration or statistic information about one specific or all HWTACACS schemes</td>
<td>display hwtacacs [hwtacacs-scheme-name [statistics]]</td>
<td>You can execute the display command in any view.</td>
</tr>
<tr>
<td>Display buffered non-response stop-accounting requests</td>
<td>display stop-accounting-buffer {hwtacacs-scheme hwtacacs-scheme-name}</td>
<td></td>
</tr>
<tr>
<td>Clear HWTACACS message statistics</td>
<td>reset hwtacacs statistics {accounting</td>
<td>authentication</td>
</tr>
<tr>
<td>Delete buffered non-response stop-accounting requests</td>
<td>reset stop-accounting-buffer {hwtacacs-scheme hwtacacs-scheme-name}</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 45: AAA CONFIGURATION

Network diagram

Figure 155  Remote RADIUS authentication of Telnet users

Internet
Telnet user
Authentication server 10.110.91.164

Configuration procedure

# Enter system view.
<5500> system-view

# Adopt AAA authentication for Telnet users.
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme
[5500-ui-vty0-4] quit

# Configure an ISP domain.
[5500] domain cams
[5500-isp-cams] access-limit enable 10
[5500-isp-cams] quit

# Configure a RADIUS scheme.
[5500] radius scheme cams
[5500-radius-cams] accounting optional
[5500-radius-cams] primary authentication 10.110.91.164 1812
[5500-radius-cams] key authentication aabbcc
[5500-radius-cams] server-type Extended
[5500-radius-cams] user-name-format with-domain
[5500-radius-cams] quit

# Associate the ISP domain with the RADIUS scheme.
[5500] domain cams
[5500-isp-cams] scheme radius-scheme cams

A Telnet user logging into the switch by a name in the format of userid @cams belongs to the cams domain and will be authenticated according to the configuration of the cams domain.
Local Authentication of FTP/Telnet Users

The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

Network requirements
In the network environment shown in Figure 156, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

Network diagram

Figure 156  Local authentication of Telnet users

![Network Diagram](image)

**Configuration procedure**
Method 1: Using local authentication scheme.

# Enter system view.

<5500> system-view

# Adopt AAA authentication for Telnet users.

[5500] user-interface vty 0 4  
[5500-ui-vty0-4] authentication-mode scheme  
[5500-ui-vty0-4] quit

# Create and configure a local user named telnet.

[5500] local-user telnet  
[5500-luser-telnet] service-type telnet  
[5500-luser-telnet] password simple aabbcc  
[5500-luser-telnet] quit

# Configure an authentication scheme for the default system domain.

[5500] domain system  
[5500-isp-system] scheme local

A Telnet user logging into the switch with the name telnet@system belongs to the system domain and will be authenticated according to the configuration of the system domain.

Method 2: using local RADIUS server

This method is similar to the remote authentication method described in "Remote RADIUS Authentication of Telnet/SSH Users". However, you need to...
Change the server IP address, and the UDP port number of the authentication server to 127.0.0.1, and 1645 respectively in the configuration step **Configure a RADIUS scheme** in “Remote RADIUS Authentication of Telnet/SSH Users”.

Enable the local RADIUS server function, set the IP address and shared key for the network access server to 127.0.0.1 and aabbcc, respectively.

Configure local users.

### Network requirements

You are required to configure the switch so that the Telnet users logging into the switch are authenticated and authorized by the TACACS server.

A TACACS server with IP address 10.110.91.164 is connected to the switch. This server will be used as the authentication and authorization server. On the switch, set both authentication and authorization shared keys that are used to exchange messages with the TACACS server to **aabbcc**. Configure the switch to strip domain names off user names before sending user names to the TACACS server.

Configure the shared key to **aabbcc** on the TACACS server for exchanging messages with the switch.

### Network diagram

**Figure 157** Remote HWTACACS authentication and authorization of Telnet users

### Configuration procedure

# Add a Telnet user.

(Omitted here)

# Configure a HWTACACS scheme.

```
<5500> system-view
[5500] hwtacacs scheme hwtac
[5500-hwtacacs-hwtac] primary authentication 10.110.91.164 49
[5500-hwtacacs-hwtac] primary authorization 10.110.91.164 49
[5500-hwtacacs-hwtac] key authentication aabbcc
[5500-hwtacacs-hwtac] key authorization aabbcc
[5500-hwtacacs-hwtac] user-name-format without-domain
[5500-hwtacacs-hwtac] quit
```

# Configure the domain name of the HWTACACS scheme to hwtac.
Troubleshooting AAA

**Troubleshooting RADIUS Configuration**

The RADIUS protocol operates at the application layer in the TCP/IP protocol suite. This protocol prescribes how the switch and the RADIUS server of the ISP exchange user information with each other.

**Symptom 1:** User authentication/authorization always fails.

**Possible reasons and solutions:**

- The user name is not in the userid@isp-name format, or the default ISP domain is not correctly specified on the switch - Use the correct user name format, or set a default ISP domain on the switch.
- The user is not configured in the database of the RADIUS server - Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password - Be sure to input the correct password.
- The switch and the RADIUS server have different shared keys - Compare the shared keys at the two ends, make sure they are identical.
- The switch cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the switch) - Take measures to make the switch communicate with the RADIUS server normally.

**Symptom 2:** RADIUS packets cannot be sent to the RADIUS server.

**Possible reasons and solutions:**

- The communication links (physical/link layer) between the switch and the RADIUS server is disconnected/blocked - Take measures to make the links connected/unblocked.
- None or incorrect RADIUS server IP address is set on the switch - Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect - Be sure to set the same UDP port numbers as those on the RADIUS server.

**Symptom 3:** The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

**Possible reasons and solutions:**

- The accounting port number is not properly set - Be sure to set a correct port number for RADIUS accounting.
- The switch requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device - Be sure to configure the RADIUS servers on the switch according to the actual situation.
Troubleshooting

HWTACACS Configuration

See the previous section if you encounter an HWTACACS problem.
**Introduction to EAD**

Endpoint Admission Defense (EAD) is an attack defense solution. Using this solution, you can enhance the active defense capability of network endpoints, prevents viruses and worms from spreading on the network, and protects the entire network by limiting the access rights of insecure endpoints.

With the cooperation of switch, AAA sever, security policy server and security client, EAD is able to evaluate the security compliance of network endpoints and dynamically control their access rights.

With EAD, a switch:

- Verifies the validity of the session control packets it receives according to the source IP addresses of the packets: It regards only those packets sourced from authentication or security policy server as valid.
- Dynamically adjusts the VLAN, rate, packet scheduling priority and Access Control List (ACL) for user terminals according to session control packets, whereby to control the access rights of users dynamically.

**Typical Network Application of EAD**

EAD checks the security status of users before they can access the network, and forcibly implements user access control policies according to the check results. In this way, it can isolate the users that are not compliant with security standard and force these users to update their virus databases and install system patches. Figure 158 shows a typical network application of EAD.
After a client passes the authentication, the security Client (software installed on the client PC) interacts with the security policy server to check the security status of the client. If the client is not compliant with the security standard, the security policy server issues an ACL to the switch, which then inhibits the client from accessing any parts of the network except for the virus/patch server.

After the client is patched and compliant with the required security standard, the security policy server reissues an ACL to the switch, which then assigns access right to the client so that the client can access more network resources.

**Configuring EAD**

The EAD configuration includes:

- Configuring the attributes of access users (such as username, user type, and password). For local authentication, you need to configure these attributes on the switch; for remote authentication, you need to configure these attributes on the AAA server.

- Configuring a RADIUS scheme.

- Configuring the IP address of the security policy server.

- Associating the ISP domain with the RADIUS scheme.

EAD is commonly used in RADIUS authentication environment.

This section mainly describes the configuration of security policy server IP address. For other related configuration, refer to “Introduction to AAA” on page 509.

Follow the steps in Table 417 to configure EAD.

**Table 417 Configuring EAD**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 417 Configuring EAD

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter RADIUS scheme view</td>
<td>radius scheme radius-scheme-name</td>
<td>—</td>
</tr>
<tr>
<td>Configure the RADIUS server type to extended</td>
<td>server-type extended</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the IP address of a security policy server</td>
<td>security-policy-server ip-address</td>
<td>Required Each RADIUS scheme supports up to eight IP addresses of security policy servers.</td>
</tr>
</tbody>
</table>

---

**EAD Configuration Example**

**Network requirements**

In Figure 159:

- A user is connected to Ethernet 1/0/1 on the switch.
- The user adopts 802.1x client supporting EAD extended function.
- You are required to configure the switch to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

The following are the configuration tasks:

- Connect the RADIUS authentication server 10.110.91.164 and the switch, and configure the switch to use port number 1812 to communicate with the server.
- Configure the authentication server type to **extended**.
- Configure the encryption password for exchanging messages between the switch and RADIUS server to **expert**.
- Configure the IP address 10.110.91.166 of the security policy server.
Configuration procedure

# Configure 802.1x on the switch. Refer to Configuring 802.1x of 802.1x Configuration.

# Configure a domain.

*5500* system-view
[5500] domain system
[5500-isp-system] quit

# Configure a RADIUS scheme.

[5500] radius scheme cams
[5500-radius-cams] primary authentication 10.110.91.164 1812
[5500-radius-cams] accounting optional
[5500-radius-cams] key authentication expert
[5500-radius-cams] server-type extended

# Configure the IP address of the security policy server.

[5500-radius-cams] security-policy-server 10.110.91.166

# Associate the domain with the RADIUS scheme.

[5500-radius-cams] quit
[5500] domain system
[5500-isp-system] radius-scheme cams
VRRP Overview

As shown in Figure 160, the following occasions may occur in a stable network:

- All the hosts in a network set the same gateway as their next hop, whose IP address is also known as the next hop address of the default route (for example, the next hop address of the default route is 10.100.10.1 in Figure 160).

- The Switch in the figure acts as the gateway of all the hosts in the network, and forwards the hosts’ packets destined for other network segments, so as to realize the communication between the hosts and the external network.

- If Switch fails, all the hosts on this segment taking Switch as the default gateway are cut off from the external network.

The networking illustrated in Figure 160 requires high stability of the default gateway. Normally, adding egress gateways is used to improve the system reliability. In this case, how to route between multiple egresses needs to be solved.

Virtual Router Redundancy Protocol (VRRP), an error-tolerant protocol defined in RFC 2338, well solves the problem mentioned above through separating physical devices and logical devices. In LANs with multicast or broadcast capabilities (such as Ethernet), VRRP can avoid single point failure through establishing backup links without modifying the configuration of dynamic routing protocols and router discovery protocols.
CHAPTER 47: VRRP CONFIGURATION

VRRP Group Introduction

VRRP allows you to combine a group of LAN switches (including a master and several backups) into a VRRP group. The VRRP group functions as a virtual router, forwarding packets as a gateway.

Figure 161  VRRP network diagram

As shown in Figure 161, a VRRP group has the following features:

- The virtual router (the VRRP group) has its own IP address (10.100.10.1 in the above figure).
- The switches within the VRRP group must have their own IP addresses (such as 10.100.10.2 for the master switch and 10.100.10.3 for the backup switch).
- Hosts in the LAN use the IP address of the virtual router (that is, 10.100.10.1) as their default gateway.
- Hosts in the LAN only know the IP address of this virtual router, that is, 10.100.10.1, but not the specific IP addresses 10.100.10.2 of the master switch and 10.100.10.3 of the backup switch.

If the master switch in the VRRP group goes down, the backup switches in the VRRP group will reelect a master switch by priority. The backup switch with the highest priority functions as the new master switch to guarantee normal communication between the hosts and the external networks.

Priority of a switch in a VRRP group

You can configure the priority of a switch in a VRRP group. A master switch is elected from these VRRP-enabled switches by priority and the remaining switches are backup switches. The master switch in a VRRP group is the one currently with the highest priority.

Switch priority ranges from 0 to 255 (a larger number indicates a higher switch priority). Note that only 1 through 254 are available to users. Switch priorities 0 and 255 are reserved for special uses and IP address owner respectively.

If an IP address owner exists in a VRRP group, you can configure a priority for the IP address owner. However your configuration will not take effect and the IP
address owner will still be the master switch of the VRRP group because the system considers the priority of the IP address owner to be 255 always.

*If two switches have the same VRRP priority, the one whose VLAN interface takes effect earlier becomes the master switch.*

### Preemptive mode and preemption delay of a switch in a VRRP group

You can configure a Switch 5500 to operate in preemptive mode.

- In non-preemptive mode, as long as a switch in a VRRP group becomes the master switch, it stays as the master as long as it operates normally, even if a backup is assigned a higher priority later.
- If all the switches in a VRRP group are set to operate in preemptive mode, a backup switch sends VRRP advertisements when it finds that its priority is higher than that of the current master switch. In this case a new election of master switch is triggered, and the backup switch becomes the master switch and the former master switch becomes a backup switch accordingly.

You can also set the preemption delay for a Switch 5500.

Setting a delay period aims at:

- In an unstable network, backup switches in a VRRP group possibly cannot receive VRRP advertisements from the master in time due to network congestions. In this case, the backup switch considers itself as the master switch and sends out VRRP advertisements to elect master switch. This causes the master of the VRRP group to be determined frequently.
- With preemption delay configured, if a backup switch does not receive VRRP advertisements from the master switch in time, it waits for a while before switching to a new master. The backup switch does not send VRRP advertisements if it receives VRRP advertisements from the master during the specified delay period.

### Authentication type and authentication key of a switch in a VRRP group

VRRP provides the following authentication types:

- **simple**: Simple text authentication. In a network under possible security threat, the authentication type can be set to `simple`. With the `simple` authentication type configured, the switch adds an authentication key into a VRRP packet before transmitting it. The receiver then compares the authentication key of the packet with the locally configured one. If they are the same, the packet will be taken as a true and legal one. Otherwise it will be regarded illegal and discarded.

- **md5**: MD5 authentication. In a vulnerable network, the authentication type can be set to `md5`. The switch then uses the authentication type provided in the Authentication Header and the local MD5 algorithm to authenticate the VRRP packets. Packets that fail to pass the authentication are discarded. The switch then sends trap messages to the NMS.

### Virtual Router Overview

#### VRRP VRRP group and virtual router IP address configuration

To create a VRRP group, you need to configure an IP address for the VRRP group virtual router. The VRRP group is automatically created after you configure the first
IP address for the VRRP group virtual router. Other IP addresses configured for the virtual router after this one are just added to the IP address list of the virtual router.

The virtual router IP address has the following features:

- The IP address of the virtual router can be an unassigned IP address in the network segment where a member switch of the VRRP group resides.

- You can specify the virtual router IP address as the IP address used by a member switch in the VRRP group. In this case, the member switch is called an IP address owner.

- The virtual router IP address and the IP addresses used by the member switches in the VRRP group must belong to the same network segment. If not, the VRRP group will be in the initial state (the state before you configure the VRRP on the switches of the group). In this case, VRRP does not take effect.

- A VRRP group is removed after all its virtual router IP addresses are removed. In this case, all the configurations performed for the VRRP group are disabled.

**Do not configure a host IP address as the IP address of the virtual router. If your host IP address is the same as the virtual router IP address of the VRRP group, all the packets sent to the current network segment will be sent to your host. As a result, packets in the network segment cannot be forwarded properly.**

**Response of the virtual router to the ping operations**

According to the standard VRRP, a running virtual router does not respond to the ping operations, so that you cannot use the ping command to check the network connectivity and whether the configuration of the IP address of a virtual router is successful.

For the Switch 5500, you can specify whether the switches in a VRRP VRRP group respond to the ping operations destined for the virtual router IP addresses.

**Mapping relationship between virtual router IP addresses and MAC addresses**

You can set the mapping between the IP address of the virtual router and the MAC addresses of the member switches of a VRRP group, so that packets sent from the hosts in the network can be forwarded to the correct gateway according to the saved MAC address forwarding table.

There are two types of mapping between the virtual router IP address and the MAC addresses:

- **Virtual router IP address-to-virtual MAC address mapping.** By default, a virtual MAC address is automatically created after a virtual router IP address is configured. Hosts send packets to gateways for layer 3 forwarding according to this virtual router MAC address. You can map multiple virtual IP addresses of the VRRP group to one virtual MAC address.

- **Virtual router IP address-to-real MAC address mapping.** When there is an IP address owner in the VRRP group, a virtual router IP address may correspond to two MAC addresses, a real MAC address of the IP address owner and a virtual MAC address created by default. In this case, you can map virtual router IP addresses to the real MAC address. Then hosts send packets to the IP address owner for layer 3 forwarding according to the real MAC address.
You need to configure the mapping between the IP addresses of the VRRP group and the MAC address before enabling VRRP feature on a Switch 5500. If VRRP is already enabled, the system does not support this configuration.

The number of virtual router IP addresses that can be mapped with the virtual router MAC address is determined by the chips of the switches in the VRRP group.

A switch can belong to multiple VRRP groups. However, the number of VRRP groups supported by a switch is determined by the chip it uses. Refer to the device specification for details.

VRRP Timer
There are two types of VRRP timer, the VRRP advertisement interval timer and the VRRP preemption delay timer.

VRRP advertisement interval timer
- The master switch advertises its normal operation state to the switches within the VRRP VRRP group by sending VRRP packets once in each specified interval (determined by the adver-interval argument).
- You can adjust the interval for a master to send VRRP advertisements by setting the VRRP advertisement interval timer. If a backup switch does not receive the VRRP advertisements from the master after a period three times of the specified interval, it considers itself as the master switch and sends out VRRP advertisements to reelect the master switch.

VRRP preemption delay timer
- The backup switch may not receive a VRRP advertisement within a period three times of the specified interval due to excessive network traffic or network instability. In this case, you can configure the VRRP preemption delay for backup switches.
- If you configure the preemption delay for a backup switch, the switch preempts the master if it does not receive a VRRP advertisement from the master after it waits for a period three times of the advertisement interval and the period specified by the preemption delay.

VRRP Tracking
If an IP address owner exists in a VRRP group, you can configure a priority for the IP address owner. However, your configuration will not take effect and the IP address owner will still be the master switch of the VRRP group because the system considers the priority of the IP address owner to be 255 always.

If an IP address owner exists in a VRRP group, the interface/port tracking function configured on the IP address owner cannot take effect.

Interface tracking function of the VRRP group
When the VLAN interface of the master switch goes down, if you want the specified backup switch to become the master, you can use the interface tracking function. With this function enabled for the VRRP group:
- If the tracked VLAN interface of the master switch goes down, the priority of the switch decreases automatically by a specified value.
The decrease of the master switch priority makes the priority of the backup switch tracking the interface become higher, and thus the backup switch becomes the new master switch.

**Port tracking function of the VRRP group**

When a physical port of the master switch goes down, if you want the specified backup switch to become the master, you can use the port tracking function. With this function enabled for the VRRP group:

- If the tracked physical port of the master switch goes down, the priority of the master switch decreases automatically by a set value.
- The decrease of the master switch priority makes the priority of the backup switch tracking the port become higher, and thus the backup switch becomes the new master switch.

**Operation Procedure of VRRP**

- With VRRP enabled, the switches determine their respective roles in a VRRP group by priority. The switch with the highest priority acts as the master switch, which will forward packets to outside networks, and the switches with lower priorities act as backup switches. The master switch sends VRRP advertisements periodically to notify that it is operating normally.
- When a backup switch receives a VRRP advertisement, it compares its own priority with that in the advertisement. If its priority is lower, it remains as a backup switch. Otherwise, it becomes the master switch.
- A backup switch starts the advertisement interval timer after it receives the advertisement to wait for the next one from the master. If the backup switch does not receive VRRP advertisements from the master switch after the timer expires, it considers that the master fails and starts the election process to elect a new master for forwarding packets.

**Periodical sending of ARP packets in a VRRP Group**

If a VRRP group exists on a network, the master switch sends gratuitous ARP packets periodically to hosts on the network, which then update their local ARP tables, ensuring that no device on this network uses the same IP address with the VRRP virtual router.

As you can create mappings between the IP address and MAC address of the VRRP virtual router, there are two cases:

- If the IP address of the virtual router corresponds to a virtual MAC address, the source MAC address in the gratuitous ARP packet will be the virtual MAC address.
- If the IP address of the virtual router corresponds to an actual MAC address, the source MAC address in the gratuitous ARP packet will be the VLAN interface’s MAC address of the master switch in the VRRP group.

For more information about ARP, refer “Configuring ARP” page 584.
VRRP Configuration

Configuring Basic VRRP Functions

Follow the steps in Table 418 to configure the basic VRRP functions:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure response of the virtual router to the ping operations</td>
<td>vrrp ping-enable</td>
<td>Optional By default, the virtual IP address cannot be pinged.</td>
</tr>
<tr>
<td>Map the virtual router IP address to a MAC address</td>
<td>vrrp method { real-mac</td>
<td>virtual-mac }</td>
</tr>
<tr>
<td>Create a VLAN</td>
<td>vlan vlan-id</td>
<td>- This operation creates the VLAN to which the VRRP group corresponds. The vlan-id argument is the ID of the VLAN.</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure a virtual router IP address</td>
<td>vrrp vrid virtual-router-id virtual-ip virtual-address</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the priority of the VRRP group</td>
<td>vrrp vrid virtual-router-id priority priority</td>
<td>Optional 100 by default.</td>
</tr>
</tbody>
</table>

It is not recommended to configure features related to VRRP group on the Layer 3 interface of a remote-probe VLAN. Otherwise, packet mirroring may be affected.

Configuring Advanced VRRP Functions

Complete these tasks to configure advanced VRRP functions

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced VRRP configuration</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the preemptive mode and preemption delay for a switch&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring VRRP authentication type and authentication key for a member switch&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring VRRP timer&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring VRRP Tracking&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Configuring the preemptive mode and preemption delay for a switch

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure a virtual router IP address</td>
<td>vrrp vrid virtual-router-id virtual-ip virtual-address</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the preemptive mode and preemption delay for the switches in the VRRP group</td>
<td>vrrp vrid virtual-router-id preempt-mode [ timer delay delay-value ]</td>
<td>Preemptive mode is set for the VRRP group by default.</td>
</tr>
</tbody>
</table>

### Configuring VRRP authentication type and authentication key for a member switch

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure a virtual router IP address</td>
<td>vrrp vrid virtual-router-id virtual-ip virtual-address</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the authentication type and authentication key</td>
<td>vrrp vrid virtual-router-id authentication-mode authentication-type authentication-key</td>
<td>Optional No authentication is performed by default.</td>
</tr>
</tbody>
</table>

### Configuring VRRP timer

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure a virtual router IP address</td>
<td>vrrp vrid virtual-router-id virtual-ip virtual-address</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the VRRP timer</td>
<td>vrrp vrid virtual-router-id timer advertise adver-interval</td>
<td>Optional 1 second by default.</td>
</tr>
</tbody>
</table>

### Configuring VRRP Tracking

Follow the steps in Table 419 to configure VRRP tracking:

**Table 419** Configuring VRRP Tracking

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
</tbody>
</table>
The port to be tracked can be in the VLAN which the VLAN interface of the VRRP group belongs to.

Up to eight ports can be tracked simultaneously through the port tracking function.

Up to eight layer 3 interfaces can be tracked through the interface tracking function.

### Single VRRP Group Configuration

**Network requirements**

Host A uses the VRRP virtual router comprising switch A and switch B as its default gateway to visit host B on the Internet.
The information about the VRRP group is as follows:

- VRRP group ID: 1
- Virtual router IP address: 202.38.160.111
- Master switch: Switch A
- Backup switch: Switch B
- Preemptive mode: enabled

### Table 420  Network description

<table>
<thead>
<tr>
<th>Switch</th>
<th>Ethernet port connecting to Host A</th>
<th>IP address of the VLAN interface</th>
<th>Switch priority in the VRRP group</th>
<th>Preemptive mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSW-A</td>
<td>Ethernet 1/0/6</td>
<td>202.38.160.1/24</td>
<td>110</td>
<td>Enabled</td>
</tr>
<tr>
<td>LSW-B</td>
<td>Ethernet 1/0/5</td>
<td>202.38.160.2/24</td>
<td>100 (default)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Network diagram

**Figure 162**  Network diagram for single-VRRP group configuration

**Configuration procedure**

- Configure Switch A.

  # Configure VLAN 3.

  ```
  [LSW-A] vlan 3
  [LSW-A-vlan3] port Ethernet1/0/10
  [LSW-A-vlan3] quit
  [LSW-A] interface Vlan-interface 3
  ```
VRRP Configuration Examples

[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
[LSW-A-Vlan-interface3] quit

# Configure VLAN 2.

<LSW-A> system-view
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-Vlan-interface2] quit

# Enable a VRRP group to respond to ping operations destined for its virtual router IP address.

[LSW-A] vrrp ping-enable

# Create a VRRP group.

[LSW-A] interface Vlan-interface 2

# Set the priority for Switch A in the VRRP group.

[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110

# Configure the preemptive mode for the VRRP group.

[LSW-A-Vlan-interface2] vrrp vrid 1 preempt-mode

By default, a VRRP group adopts the preemptive mode.

■ Configure Switch B.

# Configure VLAN 3.

[LSW-B] vlan 3
[LSW-B-vlan3] port GigabitEthernet1/0/10
[LSW-B-vlan3] quit
[LSW-B] interface Vlan-interface 3
[LSW-B-Vlan-interface3] ip address 10.100.10.3 255.255.255.0
[LSW-B-Vlan-interface3] quit

# Configure VLAN 2.

<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-Vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit

# Enable a VRRP group to respond to ping operations destined for its virtual router IP address.

[LSW-B] vrrp ping-enable
# Create a VRRP group.

```
[LSW-B] interface vlan 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Configure the preemptive mode for the VRRP group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 preempt-mode
```

The IP address of the default gateway of Host A is configured as 202.38.160.111.

Normally, Switch A functions as the gateway, but when Switch A is turned off or fails, Switch B will function as the gateway instead.

Configure Switch A to operate in preemptive mode, so that it can resume its gateway function as the master switch after recovery.

---

**VRRP Tracking Interface Configuration**

**Network requirements**

Even when Switch A is still functioning, Switch B (with another link to connect with the outside) can function as a gateway when the interface on Switch A and connecting to Internet does not function properly. This can be implemented by enabling the VLAN interface tracking function.

The VRRP group ID is set to 1, with configurations of authorization key and timer.

**Network diagram**

*Figure 163*  Network diagram for interface tracking configuration

---

**Configuration procedure**

- Configure Switch A.
# Configure VLAN 3.

[LSW-A] vlan 3  
[LSW-A-vlan3] port Ethernet1/0/10  
[LSW-A-vlan3] quit  
[LSW-A] interface Vlan-interface 3  
[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0  
[LSW-A-Vlan-interface3] quit

# Configure VLAN 2.

<LSW-A> system-view  
[LSW-A] vlan 2  
[LSW-A-vlan2] port Ethernet 1/0/6  
[LSW-A-vlan2] quit  
[LSW-A] interface Vlan-interface 2  
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0  
[LSW-A-Vlan-interface2] quit

# Configure that the virtual router can be pinged.

[LSW-A] vrrp ping-enable

# Create a VRRP group.

[LSW-A] interface Vlan-interface 2  

# Set the priority for the VRRP group.

[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110

# Set the authentication type for the VRRP group to md5, and the password to abc123.

[LSW-A-Vlan-interface2] vrrp authentication-mode md5 abc123

# Configure the master switch to send VRRP packets every 5 seconds.

[LSW-A-Vlan-interface2] vrrp vrid 1 timer advertise 5

# Set the tracked VLAN interface.

[LSW-A-Vlan-interface2] vrrp vrid 1 track interface Vlan-interface 3 reduced

■ Configure switch B.

# Configure VLAN 3.

[LSW-B] vlan 3  
[LSW-B-vlan3] port GigabitEthernet1/0/10  
[LSW-B-vlan3] quit  
[LSW-B] interface Vlan-interface 3  
[LSW-B-Vlan-interface3] ip address 10.100.10.3 255.255.255.0  
[LSW-B-Vlan-interface3] quit

# Configure VLAN 2.
<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit

# Configure that the virtual router can be pinged through.
[LSW-B] vrrp ping-enable

# Create a VRRP group.
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111

# Configure the authentication key for the VRRP group.
[LSW-B-Vlan-interface2] vrrp vrid 1 authentication-mode md5 abc123

# Configure the master to send VRRP packets every 5 seconds.
[LSW-B-Vlan-interface2] vrrp vrid 1 timer advertise 5

Normally, Switch A functions as the gateway, but when VLAN-interface 3 on Switch A goes down, its priority will be reduced by 30, lower than that of Switch B so that Switch B will preempt the master for gateway services instead.

When VLAN-interface 3 recovers, switch A will resume its gateway function as the master.

**Multiple-VRRP Group Configuration**

**Network requirements**

A switch can function as a backup switch for multiple VRRP groups.

Multiple-VRRP group configuration can implement load balancing. For example, Switch A acts as the master switch of VRRP group 1 and a backup switch in VRRP group 2. Similarly, Switch B acts as the master switch of VRRP group 2 and a backup switch in VRRP group 1. Some hosts in the network take virtual router 1 as the gateway, while others take virtual router 2 as the gateway. In this way, both load balancing and mutual backup are implemented.
Network diagram

**Figure 164** Network diagram for multiple-VRRP group configuration

![Network Diagram]

**Configuration procedure**

- Configure Switch A.

  # Configure VLAN 3.

  ```
  [LSW-A] vlan 3
  [LSW-A-vlan3] port Ethernet1/0/10
  [LSW-A-vlan3] quit
  [LSW-A] interface Vlan-interface 3
  [LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
  ```

  # Configure VLAN 2.

  ```
  <LSW-A> system-view
  [LSW-A] vlan 2
  [LSW-A-vlan2] port Ethernet 1/0/6
  [LSW-A-vlan2] quit
  [LSW-A] interface Vlan-interface 2
  [LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
  ```

  # Create VRRP group 1.

  ```
  ```

  # Set the priority for VRRP group 1.

  ```
  [LSW-A-Vlan-interface2] vrrp vrid 1 priority 150
  ```
# Create VRRP group 2.


# Configure Switch B.

# Configure VLAN 3.

[LSW-A] vlan 3
[LSW-A-vlan3] port Ethernet1/0/10
[LSW-A-vlan3] quit
[LSW-A] interface Vlan-interface 3
[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
[LSW-A-Vlan-interface3] quit

# Configure VLAN 2.

<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet1/0/6
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0

# Create VRRP group 1.

[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111

# Create VRRP group 2.

[LSW-B-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112

# Set the priority for VRRP group 2.

[LSW-B-Vlan-interface2] vrrp vrid 2 priority 110

Normally, multiple VRRP groups are used in actual use.

Network requirements

- VRRP group 1 comprises two switches, which act as the master switch and the backup switch.
- The actual IP addresses of the master and the backup switches are 10.100.10.2 and 10.100.10.3 respectively.
- The master switch is connected to the upstream network through its Ethernet 1/0/1 port. The backup switch is connected to the upstream network through its Ethernet 1/0/2 port.
- The virtual router IP address of the VRRP group is 10.100.10.1.
- Enable the port tracking function on Ethernet 1/0/1 port of the master switch and specify that the priority of the master decreases by 50 when Ethernet 1/0/1 port fails, which triggers new master switch being determined in the VRRP group 1.
Network diagram

Figure 165  Network diagram for VRRP port tracking configuration

Configuration procedure

- Configure the master switch.

  # Enter system view.

  <5500> system-view

  # Create VLAN 3.

  [5500] vlan 3
  [5500-vlan3] port Ethernet1/0/1
  [5500-vlan3] quit

  # Configure VLAN-interface 3.

  [5500] interface Vlan-interface 3
  [5500-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
  [5500-Vlan-interface3] quit

  # Create VLAN 2.

  [5500] vlan 2
  [5500-vlan2] port Ethernet1/0/1

  # Configure VLAN-interface 2.

  [5500] interface Vlan-interface 2
  [5500-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
  [5500-Vlan-interface2] quit

  # Create a VRRP group.

  [5500] interface Vlan-interface 2
  [5500-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
  [5500-vlan2] quit
# Enter Ethernet 1/0/1 port view and enable the VRRP tracking function.

```
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] vrrp Vlan-interface 2 vrid 1 track reduced 50
```

## Troubleshooting VRRP

You can locate VRRP problems through the configuration and debugging information. Here are some possible symptoms you might meet and the corresponding troubleshooting methods.

### Symptom 1: Frequent prompts of configuration errors on the console

This indicates that incorrect VRRP packets are received. It may be because of the inconsistent configuration of the switches within the VRRP group, or the attempt of other devices sending illegal VRRP packets.

- The first possible fault can be solved through modifying the configuration.
- The second possibility is caused by the malicious attempt of some devices, non-technical measures should be taken to solve the problem.

### Symptom 2: More than one master existing within a VRRP group

There are also 2 reasons. One is short coexistence of many master switches, which is normal and needs no manual intervention. Another is long coexistence of many master switches, which may be caused because the original master switch and other member switches in a VRRP group cannot receive VRRP packets from each other, or receive some illegal packets.

To solve such a problem:

- An attempt should be made to ping among these masters.
- If such an attempt fails, check the connectivity between related devices.
- If they can be pinged, check VRRP configuration.
- For the configuration of a VRRP group, complete consistency for the number of virtual IP addresses, each virtual IP address, timer interval and authentication type configured on each member switch must be guaranteed.

### Symptom 3: VRRP state of a switch changing repeatedly

Such problems occur when the VRRP group timer interval is too short. They can be solved through prolonging the interval or configuring the preemption delay period.
MAC ADDRESS AUTHENTICATION CONFIGURATION

MAC Address Authentication Overview

MAC address authentication provides a way for authenticating users based on ports and MAC addresses, without requiring any client software to be installed on the hosts. Once detecting a new MAC address, it initiates the authentication process. During authentication, the user does not need to enter username or password manually.

You can implement MAC address authentication locally or on a RADIUS server.

After determining the authentication method, users can select one of the following types of user name as required:

- MAC address mode, where the MAC address of a user serves as both the user name for authentication.
- Fixed mode, where user names and passwords are configured on a switch in advance. In this case, the user name, the password, and the limits on the total number of user names are the matching criterion for successful authentication. For details, refer to “AAA Configuration” on page 519 for information about local user attributes.

Performing MAC Address Authentication on a RADIUS Server

When authentications are performed on a RADIUS server, the switch serves as a RADIUS client and completes MAC address authentication in combination of the RADIUS server.

- In MAC address mode, the switch sends the detected MAC addresses to the RADIUS server as both the user names and passwords, or sends the detected MAC addresses to the RADIUS server as the user names and uses the configured fixed password as the password.
- In fixed mode, the switch sends the user name and password previously configured for the user to the RADIUS server for authentication.

A user can access a network upon passing the authentication performed by the RADIUS server.

Performing MAC Address Authentication Locally

When authentications are performed locally, users are authenticated by switches. In this case,

- In MAC address mode, the local user name to be configured is the MAC address of an access user while the password may be the MAC address of the user or the configured fixed password (which one is used depends on your configuration). Hyphens must or must not be included depending on the format configured with the `mac-authentication authmode usernameasmacaddress usernameformat` command; otherwise, the authentication will fail.
CHAPTER 48: MAC ADDRESS AUTHENTICATION CONFIGURATION

- In fixed mode, all users’ MAC addresses are automatically mapped to the configured local passwords and usernames.
- The service type of a local user needs to be configured as lan-access.

**Related Concepts**

**MAC Address Authentication Timers**

The following timers function in the process of MAC address authentication:

- **Offline detect timer**: At this interval, the switch checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the switch sends a stop-accounting notice to the RADIUS server.
- **Quiet timer**: Whenever a user fails MAC address authentication, the switch does not initiate any MAC address authentication of the user during a period defined by this timer.
- **Server timeout timer**: During authentication of a user, if the switch 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 from accessing the network.

**Quiet MAC Address**

When a user fails MAC address authentication, the MAC address becomes a quiet MAC address, which means that any packets from the MAC address will be discarded simply by the switch until the quiet timer expires. This prevents an invalid user from being authenticated repeatedly in a short time.

⚠️ **CAUTION**: If the quiet MAC is the same as the static MAC configured or an authentication-passed MAC, then the quiet function is not effective.

### Configuring Basic MAC Address Authentication Functions

<table>
<thead>
<tr>
<th>Table 421</th>
<th>Configure basic MAC address authentication functions</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable MAC address authentication globally</td>
<td><code>mac-authentication</code></td>
<td>Required</td>
</tr>
<tr>
<td>Enable MAC address authentication for the specified port(s) or the current port</td>
<td><code>mac-authentication interface interface-list interface-type interface-number mac-authentication quit</code></td>
<td>Use either method</td>
</tr>
<tr>
<td>Set the user name in MAC address mode for MAC address authentication</td>
<td>`mac-authentication authmode usernameasmacaddress [ usernameformat { with-hyphen</td>
<td>without-hyphen } { lowercase</td>
</tr>
</tbody>
</table>

By default, the MAC address of a user is used as the user name.
Table 421 Configure basic MAC address authentication functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Set the user name in fixed mode for MAC address authentication | mac-authentication authmode username fixed | Optional
| Configure the user name | mac-authentication authusername username | By default, the user name is mac and no password is configured. |
| Configure the password | mac-authentication authpassword password | |
| Specify an ISP domain for MAC address authentication | mac-authentication domain isp-name | Required
| Configure the MAC address authentication timers | mac-authentication timer { offline-detect offline-detect-value | quiet quiet-value | server-timeout server-timeout-value } | Optional

**CAUTION:**

- If MAC address authentication is enabled on a port, you cannot configure the maximum number of dynamic MAC address entries for that port (through the **mac-address max-mac-count** command), and vice versa.
- If MAC address authentication is enabled on a port, you cannot configure port security (through the **port-security enable** command) on that port, and vice versa.
- You can configure MAC address authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC address authentication is enabled globally.

Table 422 MAC address authentication enhanced function configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a Guest VLAN</td>
<td>Optional</td>
<td>&quot;Configuring a Guest VLAN&quot;</td>
</tr>
</tbody>
</table>
CHAPTER 48: MAC ADDRESS AUTHENTICATION CONFIGURATION

Configuring a Guest VLAN

Different from Guest VLANs described in the 802.1x and System-Guard chapters, Guest VLANs mentioned in this section refer to Guest VLANs dedicated to MAC address authentication.

After completing configuration tasks in “Configuring Basic MAC Address Authentication Functions” on page 572 for a switch, this switch can authenticate access users according to their MAC addresses or according to fixed user names and passwords. The switch will not learn MAC addresses of the clients failing in the authentication into its local MAC address table, thus prevent illegal users from accessing the network.

In some cases, if the clients failing in the authentication are required to access some restricted resources in the network (such as the virus library update server), you can use the Guest VLAN.

You can configure a Guest VLAN for each port of the switch. When a client connected to a port fails in MAC address authentication, this port will be added into the Guest VLAN automatically. The MAC address of this client will also be learned into the MAC address table of the Guest VLAN, and thus the user can access the network resources of the Guest VLAN.

After a port is added to a Guest VLAN, the switch will re-authenticate the first access user of this port (namely, the first user whose unicast MAC address is learned by the switch) periodically. If this user passes the re-authentication, this port will exit the Guest VLAN, and thus the user can access the network normally.

CAUTION:

- Guest VLANs are implemented in the mode of adding a port to a VLAN. For example, when multiple users are connected to a port, if the first user fails in the authentication, the other users can access only the contents of the Guest VLAN. The switch will re-authenticate only the first user accessing this port, and the other users cannot be authenticated again. Thus, if more than one client is connected to a port, you cannot configure a Guest VLAN for this port.

- After users that are connected to an existing port failed to pass authentication, the switch adds the port to the Guest VLAN. Therefore, the Guest VLAN can separate unauthenticated users on an access port. When it comes to a trunk port or a hybrid port, if a packet itself has a VLAN tag and be in the VLAN that the port allows to pass, the packet will be forwarded perfectly without the influence of the Guest VLAN. That is, packets can be forwarded to the VLANs other than the Guest VLAN through the trunk port and the hybrid port, even users fail to pass authentication.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the maximum number of MAC address authentication users allowed to access a port</td>
<td>Optional</td>
<td>“Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port”</td>
</tr>
</tbody>
</table>
Table 423  Configure a Guest VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><strong>interface interface-type interface-number</strong></td>
<td>-</td>
</tr>
<tr>
<td>Configure the Guest VLAN for the current port</td>
<td><strong>mac-authentication guest-vlan vlan-id</strong></td>
<td>Required By default, no Guest VLAN is configured for a port by default.</td>
</tr>
<tr>
<td>Return to system view</td>
<td><strong>quit</strong></td>
<td>-</td>
</tr>
<tr>
<td>Configure the interval at which the switch re-authenticates users in Guest VLANs</td>
<td><strong>mac-authentication timer guest-vlan-reauth interval</strong></td>
<td>Optional By default, the switch re-authenticates the users in Guest VLANs at the interval of 30 seconds by default.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- If more than one client are connected to a port, you cannot configure a Guest VLAN for this port.

- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.

- The undo vlan command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to “VLAN Configuration” on page 113 for a description of the undo VLAN command.

- Only one Guest VLAN can be configured for a port, and the VLAN configured as the Guest VLAN must be an existing VLAN. Otherwise, the Guest VLAN configuration does not take effect. If you want to change the Guest VLAN for a port, you must remove the current Guest VLAN and then configure a new Guest VLAN for this port.

- 802.1x authentication cannot be enabled for a port configured with a Guest VLAN.

- The Guest VLAN function for MAC address authentication does not take effect when port security is enabled.

Table 424  Configure the maximum number of MAC address authentication users allowed to access a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
</tbody>
</table>
CHAPTER 48: MAC ADDRESS AUTHENTICATION CONFIGURATION

CAUTION:

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to “Port Security Configuration” on page 185 the Port Security manual for a description of the port security function.

- You cannot configure the maximum number of MAC address authentication users for a port if any user connected to this port is online.

### Displaying and Maintaining MAC Address Authentication

After completing the above configuration, you can execute the **display** command in any view to display system running of MAC Address Authentication configuration, and to verify the effect of the configuration. You can execute the **reset** command in user view to clear the statistics of MAC Address Authentication.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display global or on-port information about MAC address authentication</td>
<td>display mac-authentication [ interface interface-list ]</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Clear the statistics of global or on-port MAC address authentication</td>
<td>reset mac-authentication statistics [ interface interface-type interface-number ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

### MAC Address Authentication Configuration Example

**Network requirements**

As illustrated in Figure 166, a supplicant is connected to the switch through port Ethernet 1/0/2.

- MAC address authentication is required on port Ethernet 1/0/2 to control user access to the Internet.

- All users belong to domain aabbc.jpg. The authentication performed is locally and the MAC address of the PC (00-0d-88-f6-44-c1) is used as both the user name and password.
Network Diagram

Figure 166  Network diagram for MAC address authentication configuration

```
           Ethernet 1/0/2
            
          PC                  Switch
            
MAC: 00-0d-88-f6-44-c1
```

Configuration Procedure

# Enable MAC address authentication on port Ethernet 1/0/2.

```
<5500> system-view
[5500] mac-authentication interface Ethernet 1/0/2
```

# Set the user name in MAC address mode for MAC address authentication, requiring hyphened lowercase MAC addresses as the usernames and passwords.

```
[5500] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen lowercase
```

# Add a local user.

- Specify the user name and password.

```
[5500] local-user 00-0d-88-f6-44-c1
[5500-luser-00-0d-88-f6-44-c1] password simple 00-0d-88-f6-44-c1
```

- Set the service type to **lan-access**.

```
[5500-luser-00-0d-88-f6-44-c1] service-type lan-access
[5500-luser-00-0d-88-f6-44-c1] quit
```

# Add an ISP domain named aabbcc.net.

```
[5500] domain aabbcc.net
New Domain added.
```

# Specify to perform local authentication.

```
[5500-isp-aabbcc.net] scheme local
[5500-isp-aabbcc.net] quit
```

# Specify aabbcc.net as the ISP domain for MAC address authentication

```
[5500] mac-authentication domain aabbcc.net
```

# Enable MAC address authentication globally (This is usually the last step in configuring access control related features. Otherwise, a user may be denied of access to the networks because of incomplete configuration.)

```
[5500] mac-authentication
```

After doing so, your MAC address authentication configuration will take effect immediately. Only users with the MAC address of 00-0d-88-f6-44-c1 are allowed to access the Internet through port Ethernet 1/0/2.
Introduction to ARP

ARP Function
Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.

ℹ️ Unless otherwise stated, a data link layer address in this chapter refers to a 48-bit Ethernet MAC address.

ARP Message Format
ARP messages are classified as ARP request messages and ARP reply messages. Figure 167 illustrates the format of these two types of ARP messages.

- As for an ARP request, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender requests for.
- As for an ARP reply, all the fields are set.

Figure 167 ARP message format

<table>
<thead>
<tr>
<th>Hardware type (16 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol type (16 bits)</td>
</tr>
<tr>
<td>Length of hardware address</td>
</tr>
<tr>
<td>Length of protocol address</td>
</tr>
<tr>
<td>Operator (16 bits)</td>
</tr>
<tr>
<td>Hardware address of the sender</td>
</tr>
<tr>
<td>IP address of the sender</td>
</tr>
<tr>
<td>Hardware address of the receiver</td>
</tr>
<tr>
<td>IP address of the receiver</td>
</tr>
</tbody>
</table>

Table 426 describes the fields of an ARP packet.
CHAPTER 49: ARP CONFIGURATION

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored. The Switch 5500 provides the `display arp` command to display the information about ARP mapping entries.

ARP entries in the Switch 5500 can either be static entries or dynamic entries, as described in Table 428.

**Table 426**  Description of the ARP packet fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Type</td>
<td>Type of the hardware interface. Refer to Table 427 for the information about the field values.</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Type of protocol address to be mapped. 0x0800 indicates an IP address.</td>
</tr>
<tr>
<td>Length of hardware address</td>
<td>Hardware address length (in bytes)</td>
</tr>
<tr>
<td>Length of protocol address</td>
<td>Protocol address length (in bytes)</td>
</tr>
<tr>
<td>Operator</td>
<td>Indicates the type of a data packets, which can be:</td>
</tr>
<tr>
<td></td>
<td>■ 1: ARP request packets</td>
</tr>
<tr>
<td></td>
<td>■ 2: ARP reply packets</td>
</tr>
<tr>
<td></td>
<td>■ 3: RARP request packets</td>
</tr>
<tr>
<td></td>
<td>■ 4: RARP reply packets</td>
</tr>
<tr>
<td>Hardware address of the sender</td>
<td>Hardware address of the sender</td>
</tr>
<tr>
<td>IP address of the sender</td>
<td>IP address of the sender</td>
</tr>
<tr>
<td>Hardware address of the receiver</td>
<td>For an ARP request packet, this field is null.</td>
</tr>
<tr>
<td>IP address of the receiver</td>
<td>IP address of the receiver</td>
</tr>
</tbody>
</table>

**Table 427**  Description of the values of the hardware type field

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet</td>
</tr>
<tr>
<td>2</td>
<td>Experimental Ethernet</td>
</tr>
<tr>
<td>3</td>
<td>X.25</td>
</tr>
<tr>
<td>4</td>
<td>Proteon ProNET (Token Ring)</td>
</tr>
<tr>
<td>5</td>
<td>Chaos</td>
</tr>
<tr>
<td>6</td>
<td>IEEE802.X</td>
</tr>
<tr>
<td>7</td>
<td>ARC network</td>
</tr>
</tbody>
</table>

**ARP Table**

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored. The Switch 5500 provides the `display arp` command to display the information about ARP mapping entries.

**Table 428**  ARP entries

<table>
<thead>
<tr>
<th>ARP entry</th>
<th>Generation Method</th>
<th>Maintenance Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static ARP entry</td>
<td>Manually configured</td>
<td>Manual maintenance</td>
</tr>
<tr>
<td>Dynamic ARP entry</td>
<td>Dynamically generated</td>
<td>ARP entries of this type age with time. The aging period is set by the ARP aging timer.</td>
</tr>
</tbody>
</table>
Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B. The resolution process is as follows:

1. Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, 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 source IP address and source MAC address are respectively the IP address and MAC address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process 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 into its ARP mapping 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 into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

Usually ARP dynamically implements and automatically seeks mappings from IP addresses to MAC addresses, without manual intervention.

**Man-in-the-middle attack**

According to the ARP design, after receiving an ARP response, a host adds the IP-to-MAC mapping of the sender into its ARP mapping table even if the MAC address is not the real one. This can reduce the ARP traffic in the network, but it also makes ARP spoofing possible.

In Figure 169, Host A communicates with Host C through a switch. To intercept the traffic between Host A and Host C, the hacker (Host B) forwards invalid ARP reply messages to Host A and Host C respectively, causing the two hosts to update the MAC address corresponding to the peer IP address in their ARP tables with the MAC address of Host B. Then, the traffic between Host A and C will pass through Host B which acts like a **man-in-the-middle** that may intercept and modify the
communication information. Such an attack is called the man-in-the-middle attack.

Figure 169  Network diagram for ARP man-in-the-middle attack

ARP attack detection

To guard against the man-in-the-middle attacks launched by hackers or attackers, the Switch 5500 supports the ARP attack detection function. All ARP (both request and response) packets passing through the switch are redirected to the CPU, which checks the validity of all the ARP packets by using the DHCP snooping table or the manually configured IP binding table. For description of DHCP snooping table and the manually configured IP binding table, refer to “DHCP Snooping Configuration” on page 647.

After you enable the ARP attack detection function, the switch will check the following items of an ARP packet: the source MAC address, source IP address, port number of the port receiving the ARP packet, and the ID of the VLAN the port resides. If these items match the entries of the DHCP snooping table or the manual configured IP binding table, the switch will forward the ARP packet; if not, the switch discards the ARP packet.

- With trusted ports configured, ARP packets coming from the trusted ports will not be checked, while those from other ports will be checked through the DHCP snooping table or the manually configured IP binding table.
- With the ARP restricted forwarding function enabled, ARP request packets are forwarded through trusted ports only; ARP response packets are forwarded according to the MAC addresses in the packets, or through trusted ports if the MAC address table contains no such destination MAC addresses.

Introduction to ARP Packet Rate Limit

To prevent the man-in-the-middle attack, a switch enabled with the ARP attack detection function delivers ARP packets to the CPU to check the validity of the packets. However, this causes a new problem: If an attacker sends a large number of ARP packets to a port of a switch, the CPU will get overloaded, causing other functions to fail, and even the whole device to break down. To guard against such
an attacks, the Switch 5500 support the ARP packets rate limit function, which will shut down the attacked port, thus preventing serious impact on the CPU.

With this function enabled on a port, the switch will count the ARP packets received on the port within each second. If the number of ARP packets received on the port per second exceeds the preconfigured value, the switch considers that the port is attacked by ARP packets. In this case, the switch will shut down the port. As the port does not receive any packet, the switch is protected from the ARP packet attack.

At the same time, the switch supports automatic recovery of port state. If a port is shut down by the switch due to high packet rate, the port will revert to the Up state after a configured period of time.

The following are the characteristics of gratuitous ARP packets:

- Both source and destination IP addresses carried in a gratuitous ARP packet are the local addresses, and the source MAC address carried in it is the local MAC addresses.
- If a device finds that the IP addresses carried in a received gratuitous packet conflict with those of its own, it returns an ARP response to the sending device to notify of the IP address conflict.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflicts exist between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

With the gratuitous ARP packet learning function enabled, upon receiving a gratuitous ARP packet, a switch that does not have the corresponding ARP entry adds the information contained in the gratuitous ARP packet into its ARP table.

**Periodical sending of gratuitous ARP packets**

*This section applies to the Switch 5500 only; not the Switch 5500G.*

In an actual network, when the network load or the CPU occupancy of the receiving host is high, ARP packets may be lost or the host may be unable to timely process the ARP packets received. In such a case, the dynamic ARP entries on the receiving host may age out, and the traffic between the host and the sending device will get interrupted before the host learns the MAC address of the sending device again and installs a corresponding entry in the ARP table.

To address this issue, by default, the Switch 5500 allows VLAN interfaces to send gratuitous ARP packets periodically. That is, as long as a VLAN interface is in the Up state, it sends gratuitous ARP packets at an interval of 30 seconds so that the receiving host can refresh the MAC address of the switch in the ARP table timely, thereby preventing traffic interruption mentioned above.
**Periodical sending of ARP packets in a VRRP backup group**

*This section applies to the Switch 5500 only; not the Switch 5500G.*

If a VRRP backup group exists on a network, the master switch sends gratuitous ARP packets periodically to hosts on the network, which then update their local ARP tables, ensuring that no device on this network uses the same IP address with the VRRP virtual router.

As you can create mappings between the IP address and MAC address of the VRRP virtual router, there are two cases:

- If the IP address of the virtual router corresponds to a virtual MAC address, the source MAC address in the gratuitous ARP packet will be the virtual MAC address.
- If the IP address of the virtual router corresponds to an actual MAC address, the source MAC address in the gratuitous ARP packet will be the VLAN interface’s MAC address of the master switch in the VRRP backup group.

---

### Configuring ARP

#### Configuring ARP Basic Functions

<table>
<thead>
<tr>
<th>Table 429</th>
<th>Configure ARP basic functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Add a static ARP entry</td>
<td>arp static ip-address mac-address [ vlan-id interface-type interface-number ]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:**

- Static ARP entries are valid as long as the Ethernet switch operates normally. But some operations, such as removing a VLAN, or removing a port from a VLAN, will make the corresponding ARP entries invalid and therefore removed automatically.

- As for the `arp static` command, the value of the `vlan-id` argument must be the ID of an existing VLAN, and the port identified by the `interface-type` and `interface-number` arguments must belong to the VLAN.

- Currently, static ARP entries cannot be configured on the ports of an aggregation group.
Configuring ARP Attack Detection

Table 430 Configure the ARP attack detection function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable DHCP snooping</td>
<td>dhcp-snooping</td>
<td>Required By default, the DHCP snooping function is disabled.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Specify the current port as a trusted port</td>
<td>dhcp-snooping trust</td>
<td>Required By default, after DHCP snooping is enabled, all ports of a switch are untrusted ports.</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable the ARP attack detection function</td>
<td>arp detection enable</td>
<td>Required By default, ARP attack detection is disabled on all ports.</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the port as an ARP trusted port</td>
<td>arp detection trust</td>
<td>Optional By default, a port is an untrusted port.</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN view</td>
<td>vlan vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Enable ARP restricted forwarding</td>
<td>arp restricted-forwarding enable</td>
<td>Optional By default, the ARP restricted forwarding function is disabled. The device forwards legal ARP packets through all its ports.</td>
</tr>
</tbody>
</table>

- You need to enable DHCP snooping and configure DHCP snooping trusted ports on the switch before configuring the ARP attack detection function. For more information about DHCP snooping, refer to “DHCP Snooping Configuration” on page 647.
- Currently, the VLAN ID of an IP-to-MAC binding configured on a port of a Switch 5500 is the same as the default VLAN ID of the port. If the VLAN tag of an ARP packet is different from the default VLAN ID of the receiving port, the ARP packet cannot pass the ARP attack detection based on the IP-to-MAC bindings.
- Generally, the uplink port of a switch is configured as a trusted port.
- Before enabling ARP restricted forwarding, make sure you enable ARP attack detection and configure ARP trusted ports.
- You are not recommended to configure ARP attack detection on the ports of a fabric or an aggregation group.
Configuring the ARP Packet Rate Limit Function

- You need to enable the port state auto-recovery feature before you can configure the port state auto-recovery interval.
- You are not recommended to configure the ARP packet rate limit function on the ports of an aggregation group.

<table>
<thead>
<tr>
<th>Table 431</th>
<th>Configure the ARP packet rate limit function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Enable the ARP packet rate limit function</td>
<td>arp rate-limit enable</td>
</tr>
<tr>
<td>Configure the maximum ARP packet rate allowed on the port</td>
<td>arp rate-limit rate</td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
</tr>
<tr>
<td>Enable the port state auto-recovery function</td>
<td>arp protective-down recover enable</td>
</tr>
<tr>
<td>Configure the port state auto-recovery interval</td>
<td>arp protective-down recover interval interval</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 432</th>
<th>Configure the gratuitous ARP packet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable the gratuitous ARP packet learning function</td>
<td>gratuitous-arp-learning enable</td>
</tr>
<tr>
<td>Enable the master switch of a VRRP backup group to send gratuitous ARP packets periodically</td>
<td>arp send-gratuitous enable vrrp</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
</tr>
</tbody>
</table>
The sending of gratuitous ARP packets is enabled as long as a Switch 5500 operates. No command is needed for enabling this function. That is, the device sends gratuitous ARP packets whenever a VLAN interface is enabled (such as when a link is enabled or an IP address is configured for the VLAN interface) or whenever the IP address of a VLAN interface is changed.

Before enabling the master switch of a VRRP backup group to send gratuitous ARP packets periodically, you need to create the VRRP backup group and perform corresponding configurations. Refer to the section entitled “VRRP Configuration” on page 559 for details.

Displaying and Debugging ARP

After completing the above configuration, you can execute the display command in any view to display the running of the ARP configuration, and to verify the effect of the configuration. You can execute the reset command in user view to clear ARP entries.

### Table 432 Configure the gratuitous ARP packet

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the VLAN interface to send gratuitous ARP packets periodically</td>
<td>gratuitous-arp period-sending enable</td>
<td>Optional By default, the VLAN interface of the switch is enabled to send gratuitous ARP packets periodically.</td>
</tr>
</tbody>
</table>

### Table 433 Display and debug ARP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display specific ARP mapping table entries</td>
<td>display arp static</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Display the ARP mapping entries related to a specified string in a specified way</td>
<td>display arp dynamic static { begin</td>
<td>include</td>
</tr>
<tr>
<td>Display the number of the ARP entries of a specified type</td>
<td>display arp count dynamic static [ { begin</td>
<td>include</td>
</tr>
<tr>
<td>Display the statistics about the untrusted ARP packets dropped by the specified port</td>
<td>display arp detection statistics interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Display the setting of the ARP aging timer</td>
<td>display arp timer aging</td>
<td></td>
</tr>
<tr>
<td>Clear specific ARP entries</td>
<td>reset arp dynamic static interface interface-type interface-number</td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>

### ARP Configuration Example

#### ARP Basic Configuration Example

**Network requirement**

- Disable the ARP entry check on the switch.
- On the Switch 5500 (not necessary for the Switch 5500G), disable VLAN interface 1 from sending gratuitous ARP packets periodically.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Add a static ARP entry, with the IP address being 192.168.1.1, the MAC address being 000f-e201-0000, and the outbound port being Ethernet 1/0/10 of VLAN 1.

Configuration procedure

```shell
<5500> system-view
[5500] undo arp check enable
[5500] interface vlan 1
[5500-Vlan-interface1] undo gratuitous-arp period-resending enable
[5500-Vlan-interface1] quit
[5500] undo gratuitous-arp period-sending enable
[5500] arp timer aging 10
[5500] arp static 192.168.1.1 000f-e201-0000 1 Ethernet 1/0/10
```

ARP Attack Detection
and Packet Rate Limit
Configuration Example

Network requirements

As shown in Figure 170, Ethernet 1/0/1 of Switch A connects to DHCP Server; Ethernet 1/0/2 connects to Client A, Ethernet 1/0/3 connects to Client B. Ethernet 1/0/1, Ethernet 1/0/2 and Ethernet 1/0/3 belong to VLAN 1.

- Enable DHCP snooping on Switch A and specify Ethernet 1/0/1 as the DHCP snooping trusted port.
- Enable ARP attack detection in VLAN 1 to prevent ARP man-in-the-middle attacks, and specify Ethernet 1/0/1 as the ARP trusted port.
- Enable the ARP packet rate limit function on Ethernet 1/0/2 and Ethernet 1/0/3 of Switch A, so as to prevent Client A and Client B from attacking Switch A through ARP traffic.
- Enable the port state auto recovery function on the ports of Switch A, and set the recovery interval to 200 seconds.

Network diagram

**Figure 170**  ARP attack detection and packet rate limit configuration
Configuration procedure

# Enable DHCP snooping on Switch A.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

# Specify Ethernet 1/0/1 as the DHCP snooping trusted port and the ARP trusted port.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] dhcp-snooping trust
[SwitchA-Ethernet1/0/1] arp detection trust
[SwitchA-Ethernet1/0/1] quit
```

# Enable ARP attack detection on all ports in VLAN 1.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
[SwitchA-vlan1] quit
```

# Enable the ARP packet rate limit function on Ethernet 1/0/2, and set the maximum ARP packet rate allowed on the port to 20 pps.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] arp rate-limit enable
[SwitchA-Ethernet1/0/2] arp rate-limit 20
[SwitchA-Ethernet1/0/2] quit
```

# Enable the ARP packet rate limit function on Ethernet 1/0/3, and set the maximum ARP packet rate allowed on the port to 50 pps.

```
[SwitchA] interface Ethernet 1/0/3
[SwitchA-Ethernet1/0/3] arp rate-limit enable
[SwitchA-Ethernet1/0/3] arp rate-limit 50
[SwitchA-Ethernet1/0/3] quit
```

# Configure the port state auto recovery function, and set the recovery interval to 200 seconds.

```
[SwitchA] arp protective-down recover enable
[SwitchA] arp protective-down recover interval 200
```
Proxy ARP Configuration

Proxy ARP Overview

Introduction to Proxy ARP

For a host ARP request on a network to be forwarded to an interface that is on the same network, but isolated at Layer 2, or a host on another network, the device connecting the two physical or virtual networks must be able to respond to the request. This is achieved by proxy ARP.

Work Mechanism of Proxy ARP

As shown in Figure 171, Host A and Host D are on different sub networks. When Host A (192.168.0.22/16) needs to send packets to Host D (192.168.1.30/16), because the mask of the two hosts are both 16 bits, Host A regards Host D to be on its directly connected sub network, and thus Host A will broadcast an ARP request to request the MAC address of Host D.

- When the proxy ARP feature is not enabled on the switch, because Host A and Host D are in different VLANs, the ARP request sent by Host A cannot reach Host D, and the two hosts cannot communicate.
- With proxy ARP enabled on the switch, when VLAN-interface 3 receives the ARP request, if the switch finds a route to the destination IP address (encapsulated in the ARP request) in the routing table, the switch sends host A the MAC address of VLAN-interface 3 in an ARP response (with the source IP address being the destination IP address of the ARP request). After receiving the ARP response, Host A creates an ARP entry, in which the destination IP address is the IP address of Host D (192.168.1.30/16), and the MAC address is
that of VLAN-interface 3. The following packets sent from Host A to Host D will all be sent to VLAN-interface 3 of the switch, and then the switch forwards the packets in Layer 3 to Host D, so as to realize the Layer 3 connectivity between Host A and Host D.

### Configuring Proxy ARP

<table>
<thead>
<tr>
<th>Table 434</th>
<th>Configure proxy ARP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface Vlan-interface vlan-id</code></td>
</tr>
<tr>
<td>Enable proxy ARP</td>
<td><code>arp proxy enable</code></td>
</tr>
<tr>
<td>Display the proxy ARP configuration</td>
<td><code>display arp proxy [ interface Vlan-interface vlan-id ]</code></td>
</tr>
</tbody>
</table>

### Network requirements

- The IP address of Host A is 192.168.0.22/16, and that of Host D is 192.168.1.30/16.
- Create VLAN 3 and VLAN 4 on the switch.
- The IP address of VLAN-interface 3 is 192.168.0.27/24, and that of VLAN-interface 4 is 192.168.1.27/24.
- Enable proxy ARP on VLAN-interface 3 and VLAN-interface 4 to realize the communication between Host A and Host D.

### Network diagram

*Figure 172*  Network diagram for proxy ARP
Configuration procedure

# Configure the IP address of VLAN-interface 3 to be 192.168.0.27/24.

```plaintext
<Switch> system-view
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] ip address 192.168.0.27 24
[Switch-Vlan-interface3] quit
```

# Configure the IP address of VLAN-interface 4 to be 192.168.1.27/24.

```plaintext
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] ip address 192.168.1.27 24
[Switch-Vlan-interface4] quit
```

# Enter VLAN-interface 3 view, and enable proxy ARP on it.

```plaintext
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] arp proxy enable
[Switch-Vlan-interface3] quit
```

# Enter VLAN-interface 4 view, and enable proxy ARP on it.

```plaintext
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] arp proxy enable
[Switch-Vlan-interface4] quit
```

Network requirements

- Switch A (a Switch 5500 ) is connected to Switch B through Ethernet 1/0/1.
- Ethernet 1/0/2 and Ethernet 1/0/3 on Switch B belong to VLAN 1, and are connected to Host A and Host B respectively.
- Host A and Host B isolated at Layer 2 can communicate at Layer 3 through Switch A.

Network diagram

Figure 173  Network diagram for Proxy ARP configuration in port isolation application

Configuration procedure

1 Configure Switch B

# Add Ethernet 1/0/2 and Ethernet 1/0/3 into an isolation group, disabling Host A and Host B from communicating with each other at Layer 2.
For details on port isolation, refer to the section entitled “Port Isolation Configuration” on page 181.

```yaml
<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port isolate
[SwitchB-Ethernet1/0/2] quit
[SwitchB] interface Ethernet 1/0/3
[SwitchB-Ethernet1/0/3] port isolate
[SwitchB-Ethernet1/0/3] quit
```

2 Configure Switch A

```bash
# Configure proxy ARP on VLAN-interface 1, enabling Host A and Host B to communicate at Layer 3.

<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] arp proxy enable
[SwitchA-Vlan-interface1] quit
```
RESILIENT ARP CONFIGURATION

Resilient ARP Introduction

In intelligent resilient framework (IRF) network application, normally you need to connect redundancy links between the fabric and other devices to support the resilient network. But if the connections inside the fabric break off, the fabric splits. In this case, the redundancy link may connect with two or more Layer 3 devices with the same configurations in the same network. Thus these devices operate the same routing function. Adopting the Resilient ARP function can avoid this. Resilient ARP can find whether there are the same Layer 3 devices in the network. If so, it keeps one device as the Layer 3 device, and changes the other devices to be the Layer 2 devices.

The state machine of Resilient ARP has six states which are Initialize, ListenForL3Master, L3Master, L3slave, L2Master, and L2slave. L3Master sends Resilient ARP packets periodically to notify other fabrics that the local fabric is in the Layer 3 state.

Resilient ARP implements the system state switching by sending/receiving Resilient ARP packets periodically, so as to determine a device to work as a Layer 3 device or a Layer 2 device.

Configuring Resilient ARP

Resilient ARP configuration includes:

- Enable/disable the Resilient ARP function.

When Resilient ARP function is enabled, the system can deal with the devices according to the current state. When the connections inside a fabric break off, Resilient ARP can send Resilient ARP packets through the VLAN interface where the redundancy link resides, so as to determine a device to work as a Layer 3 device or as a Layer 2 device.

- Configure the VLAN interface through which Resilient packets are sent.

You can use the following commands to configure the VLAN interface through which Resilient packets are sent. When no VLAN interface is specified, Resilient packets are sent through the default VLAN interface.

<table>
<thead>
<tr>
<th>Table 435</th>
<th>Configure the Resilient ARP function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| Enable the Resilient ARP function | resilient-arp enable | Required
|                        |                          | By default, the Resilient ARP function is enabled. |
Note that the above configuration specifies the VLAN interface through which Resilient packets are sent, whereas all the VLAN interfaces can receive Resilient ARP packets.

**Table 435  Configure the Resilient ARP function**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the VLAN interface through which Resilient packets are sent</td>
<td>resilient-arp interface vlan-interface vlan-id</td>
<td>Optional By default, Resilient ARP packets are sent through the interface of VLAN 1(VLAN-interface 1).</td>
</tr>
<tr>
<td>Display information about the Resilient ARP state</td>
<td>display resilient-arp [ unit unit-id ]</td>
<td>You can execute the display command in any view</td>
</tr>
</tbody>
</table>

Resilient ARP Configuration Example

Network requirements

There are four units in an IRF network: unit 1 to unit 4. Unit 1 and unit 3 connect to another switch (Switch) through link aggregation. If the connection between unit 1 and unit 3 and the connection between unit 2 and unit 4 break off, there will be two Layer 3 switches with the same configuration in the network. In this case, problems occur in packets forwarding between the fabric and the Switch. You can enable the Resilient ARP function for the fabric to avoid the problems. The ports through which unit 3 and unit 4 connect to the Switch belong to VLAN 2.

Network diagram

**Figure 174  Network diagram for Resilient ARP**

Configuration procedure

# Enable the Resilient ARP function.

<5500> system-view
[5500] resilient-arp enable

# Configure the Resilient ARP packets to be sent through the VLAN-interface 2.

[5500] resilient-arp interface Vlan-interface 2
**DHCP OVERVIEW**

**DHCP Introduction**

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic Host Configuration Protocol (DHCP) is developed to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Figure 175.

![Figure 175 Typical DHCP application](image)

**DHCP IP Address Assignment**

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

- **Manual assignment.** The administrator configures static IP-to-MAC bindings for some special clients, such as a WWW server. Then the DHCP server assigns these fixed IP addresses to the clients.

- **Automatic assignment.** The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.
Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1. Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.

2. Offer: In this phase, the DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER packet from the DHCP client, it chooses an unassigned IP address from the address pool according to the priority order of IP address assignment and then sends the IP address and other configuration information together in a DHCP-OFFER packet to the DHCP client. The sending mode is decided by the flag filed in the DHCP-DISCOVER packet, refer to “DHCP Packet Format” on page 599 for details.

3. Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.

4. Acknowledge: In this phase, the DHCP servers acknowledge the IP address. Upon receiving the DHCP-REQUEST packet, only the selected DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

- After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within 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.

- If there are multiple DHCP servers, IP addresses offered by other DHCP servers are assignable to other clients.

Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.
If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP servers again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described above.

### DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following figure describes the packet format (the number in the brackets indicates the field length, in bytes):

**Figure 176** DHCP packet format

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>op</td>
<td>Operation types of DHCP packets, 1 for request packets and 2 for response packets.</td>
</tr>
<tr>
<td>htype, hlen</td>
<td>Hardware address type and length of the DHCP client.</td>
</tr>
<tr>
<td>hops</td>
<td>Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.</td>
</tr>
<tr>
<td>xid</td>
<td>Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.</td>
</tr>
<tr>
<td>secs</td>
<td>Elapsed time after the DHCP client initiates a DHCP request.</td>
</tr>
<tr>
<td>flags</td>
<td>The first bit is the broadcast response flag bit, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). Other bits are reserved.</td>
</tr>
<tr>
<td>ciaddr</td>
<td>IP address of a DHCP client.</td>
</tr>
<tr>
<td>yiaddr</td>
<td>IP address that the DHCP server assigns to a client.</td>
</tr>
<tr>
<td>siaddr</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>giaddr</td>
<td>IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.</td>
</tr>
<tr>
<td>chaddr</td>
<td>Hardware address of the DHCP client.</td>
</tr>
</tbody>
</table>

The fields are described as follows:

- **op**: Operation types of DHCP packets, 1 for request packets and 2 for response packets.
- **htype**, **hlen**: Hardware address type and length of the DHCP client.
- **hops**: Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.
- **xid**: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- **secs**: Elapsed time after the DHCP client initiates a DHCP request.
- **flags**: The first bit is the broadcast response flag bit, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). Other bits are reserved.
- **ciaddr**: IP address of a DHCP client.
- **yiaddr**: IP address that the DHCP server assigns to a client.
- **siaddr**: IP address of the DHCP server.
- **giaddr**: IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.
- **chaddr**: Hardware address of the DHCP client.
- **sname**: Name of the DHCP server.
- **file**: Path and name of the boot configuration file that the DHCP server specifies for the DHCP client.
- **option**: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

**Protocol Specification**

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC3046: DHCP Relay Agent Information option
Currently, the interface-related DHCP server configurations can only be made on VLAN interfaces.

**Introduction to DHCP Server**

**Usage of DHCP Server**

Generally, DHCP servers are used in the following networks to assign IP addresses:

- Large-sized networks, where manual configuration method bears heavy load and is difficult to manage the whole network in centralized way.
- Networks where the number of available IP addresses is less than that of the hosts. In this type of networks, IP addresses are not enough for all the hosts to obtain a fixed IP address, and the number of on-line users is limited (such is the case in an ISP network). In these networks, a great number of hosts must dynamically obtain IP addresses through DHCP.
- Networks where only a few hosts need fixed IP addresses and most hosts do not need fixed IP addresses.

**DHCP Address Pool**

A DHCP address pool holds the IP addresses to be assigned to DHCP clients. When a DHCP server receives a DHCP request from a DHCP client, it selects an address pool depending on the configuration, picks an IP address from the pool and sends the IP address and other related parameters (such as the IP address of the DNS server, and the lease time of the IP address) to the DHCP client.

**Types of address pool**

The address pools of a DHCP server fall into two types: global address pool and interface address pool.

- A global address pool is created by executing the `dhcp server ip-pool` command in system view. It is valid on the current device.
- If an interface is configured with a valid unicast IP address, you can create an interface-based address pool for the interface by executing the `dhcp select interface` command in interface view. The IP addresses an interface address pool holds belong to the network segment the interface resides in and are available to the interface only.

**Structure of an address pool**

The address pools of a DHCP server are hierarchically organized in a tree-like structure. The root holds the IP address of the natural network segment, the branches hold the subnet IP addresses, and the leaves holds the IP addresses that are manually bound to specific clients. The address pools that are of the same level
are sorted by their configuration precedence order. Such a structure enables configurations to be inherited. That is, the configurations of the natural network segment can be inherited by its subnets, whose configurations in turn can be inherited by their client address. So, for the parameters that are common to the whole network segment or some subnets (such as domain name), you just need to configure them on the network segment or the corresponding subnets. The following is the details of configuration inheritance.

1. A newly created child address pool inherits the configurations of its parent address pool.

2. For an existing parent-child address pool pair, when you performs a new configuration on the parent address pool:
   - The child address pool inherits the new configuration if there is no corresponding configuration on the child address pool.
   - The child address pool does not inherit the new configuration if there is already a corresponding configuration on the child address pool.

   *The IP address lease does not enjoy the inheritance attribute.*

**Principles of address pool selection**

The DHCP server observes the following principles to select an address pool to assign an IP address to a client:

1. If the receiving interface works in the global address pool mode, the DHCP server assigns an IP address from the global address pool to the DHCP client.

2. If the receiving interface works in the interface address pool mode, the DHCP server assigns an IP address from the interface address pool to the DHCP client directly connected to the interface. If there is no available IP address in the interface address pool, the DHCP server selects an IP address from the global address pool that contains the interface address pool’s network segment for the client.

The DHCP server assigns an IP address to the client in the following order from an interface address pool or a global address pool:

1. If there is an address pool where an IP address is statically bound to the MAC address or ID of the client, the DHCP server will select this address pool and assign the statically bound IP address to the client.

2. Otherwise, the DHCP server observes the following principles to select a dynamic address pool.
   - If the client and the server reside in the same network segment, the smallest address pool that contains the IP address of the receiving interface will be selected.
   - If the client and the server do not reside in the same network segment (that is, a DHCP relay agent is in-between), the smallest address pool that contains the IP address specified in the giaddr field of the client’s request will be selected.
   - If no assignable IP address is available in the selected address pool, the DHCP server will not assign any IP address to the client because it cannot assign an IP address from the parent address pool to the client.
A DHCP server assigns IP addresses in interface address pools or global address pools to DHCP clients in the following sequence:

1. IP addresses that are statically bound to the MAC addresses of DHCP clients or client IDs.
2. The IP address that was ever assigned to the client.
3. The IP address designated by the Option 50 field in a DHCP-DISCOVER message.
4. The first assignable IP address found in a proper DHCP address pool.
5. If no IP address is available, the DHCP server queries lease-expired and conflicted IP addresses. If the DHCP server finds such IP addresses, it assigns them; otherwise the DHCP server does not assign an IP address.

In an IRF (intelligent resilient framework) system, DHCP servers operate in a centralized way to fit the IRF environment.

- DHCP servers run (as tasks) on all the units (including the master unit and the slave units) in a Fabric system. But only the one running on the master unit receives/sends packets and carries out all functions of a DHCP server. Those running on the slave units only operate as the backup tasks of the one running on the master unit.
- When a slave unit receives a DHCP-REQUEST packet, it redirects the packet to the DHCP server on the master unit, which returns a DHCP-ACK or DHCP-NAK packet to the DHCP client and at the same time backs up the related information to the slave units. In this way, when the current master unit fails, one of the slaves can change to the master and operates as the DHCP server immediately.
- DHCP is an UDP-based protocol operating at the application layer. When a DHCP server in a fabric system runs on a Layer 2 network device, DHCP packets are directly forwarded by hardware instead of being delivered to the DHCP server, or being redirected to the master unit by UDP HELPER. This idles the DHCP server. DHCP packets can be redirected to the DHCP server on the master unit by UDP HELPER only when the Layer 2 device is upgraded to a Layer 3 device.

**CAUTION:**
- When you merge two or more IRF systems into one IRF system, a new master unit is elected, and the new IRF system adopts new configurations accordingly. This may result in the existing system configurations (including the address pools configured for the DHCP servers) being lost. As the new IRF system cannot inherit the original DHCP server configurations, you need to perform DHCP server configurations for it.
- When an IRF system is split into multiple new IRF systems, some of the new IRF systems may be degraded to Layer 2 devices. For a new IRF system degraded to Layer 2 device, although the original DHCP server still exists in the new system, it runs idle for being unable to receive any packets. When the IRF system restores to a Layer 3 device due to being merged into a new IRF system, it adopts the configurations on the new IRF system. And you need to perform DHCP server configurations if the new IRF system does not have DHCP server-related configurations.
In an IRF system, the UDP HELPER function must be enabled on the DHCP servers that are in fabric state.

### DHCP Server Configuration Task List

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Enabling DHCP&quot; on page 604</td>
<td>Required</td>
</tr>
<tr>
<td>Configure address pool based DHCP server</td>
<td>One of the two options is required.</td>
</tr>
<tr>
<td>&quot;Configuring the Global Address Pool Based DHCP Server&quot; on page 605</td>
<td></td>
</tr>
<tr>
<td>&quot;Configuring the Interface Address Pool Based DHCP Server&quot; on page 614</td>
<td></td>
</tr>
<tr>
<td>&quot;Configuring DHCP Server Security Functions&quot; on page 623</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring DHCP Accounting Functions&quot; on page 624</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Enabling the DHCP Server to Process Option 82&quot; on page 625</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Enabling DHCP

You need to enable DHCP to make other related configurations take effect.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>dhcp enable</td>
<td>Optional By default, DHCP is enabled.</td>
</tr>
</tbody>
</table>

To improve security and avoid malicious attacks to unused sockets, Switch 5500s provide the following functions:

- UDP port 67 and UDP port 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP port 67 and UDP port 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After DHCP is enabled with the `dhcp enable` command, if the DHCP server and DHCP relay agent functions are not configured, UDP port 67 and UDP port 68 ports are kept disabled; if the DHCP server or DHCP relay agent function is configured, UDP port 67 and UDP port 68 ports are enabled.
- After DHCP is disabled with the `undo dhcp enable` command, even if the DHCP server or DHCP relay function is configured, UDP port 67 and UDP port 68 ports will be disabled.
Configuring the Global Address Pool Based DHCP Server

Configuration Task List

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Enabling the Global Address Pool Mode on Interface(s)&quot; on page 605</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Creating a DHCP Global Address Pool&quot; on page 606</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring an Address Allocation Mode for the Global Address Pool&quot; on page 606</td>
<td>One of the two options is required. Only one mode can be selected for the same global address pool.</td>
</tr>
<tr>
<td>&quot;Configuring the static IP address allocation mode&quot; on page 606</td>
<td></td>
</tr>
<tr>
<td>&quot;Configuring the dynamic IP address allocation mode&quot; on page 607</td>
<td></td>
</tr>
<tr>
<td>&quot;Configuring a Domain Name Suffix for the DHCP Client&quot; on page 608</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring DNS Servers for the DHCP Client&quot; on page 609</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring WINS Servers for the DHCP Client&quot; on page 609</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Gateways for the DHCP Client&quot; on page 610</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring BIMS Server Information for the DHCP Client&quot; on page 610</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Option 184 Parameters for the Client with Voice Service&quot; on page 611</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the TFTP Server and Bootfile Name for the DHCP Client&quot; on page 613</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Self-Defined DHCP Option&quot; on page 614</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configure the global address pool mode on interface(s)

You can configure the global address pool mode on the specified or all interfaces of a DHCP server. After that, when the DHCP server receives DHCP packets from DHCP clients through these interfaces, it assigns IP addresses in the global address pool to the DHCP clients.

Table 439 Configure the global address pool mode on interface(s)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Configure the specified interface(s) or all the interfaces to operate in global address pool mode | interface interface-type interface-number | Optional By default, the interface operates in global address pool mode.  
| Configure the current interface                                           | dhcp select global           | quit                                            |
| Configure multiple interfaces simultaneously in system view               | dhcp select global {          |                                                 |
|                                                                            | interface interface-type     |                                                 |
|                                                                            | interface-number, to         |                                                 |
|                                                                            | interface-type, interface-  |                                                 |
|                                                                            | number                        |                                                 |
|                                                                            | all                           |                                                 |
Creating a DHCP Global Address Pool

<table>
<thead>
<tr>
<th>Table 440</th>
<th>Create a DHCP address pool</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Create a DHCP global address pool and enter its view</td>
<td><code>dhcp server ip-pool pool-name</code></td>
</tr>
<tr>
<td>Not created by default.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring an Address Allocation Mode for the Global Address Pool

You can configure either the static IP address allocation mode or the dynamic IP address allocation mode for a global address pool, and only one mode can be configured for one DHCP global address pool.

For dynamic IP address allocation, you need to specify the range of the IP addresses to be dynamically assigned. But for static IP address binding, you can regard that the IP address statically bound to a DHCP client comes from a special DHCP address pool that contains only one IP address.

**Configuring the static IP address allocation mode**

Some DHCP clients, such as WWW servers, need fixed IP addresses. This can be achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client requests an IP address, the DHCP server searches for the IP address corresponding to the MAC address of the DHCP client and assigns the IP address to the DHCP client.

When some DHCP clients send DHCP-DISCOVER packets to the DHCP server to apply for IP addresses, they construct client IDs and add them in the DHCP-DISCOVER packets. If the bindings of client IDs and IP addresses are configured on the DHCP server, when such a client requests an IP address, the DHCP server will find the corresponding IP address based on the client ID and assign it to the DHCP client.

Currently, only one IP address in a global DHCP address pool can be statically bound to a MAC address or a client ID.

<table>
<thead>
<tr>
<th>Table 441</th>
<th>Configure to assign IP addresses by static binding</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td><code>dhcp server ip-pool pool-name</code></td>
</tr>
<tr>
<td>Configure an IP address to be statically bound</td>
<td><code>static-bind ip-address ip-address [ mask mask ]</code></td>
</tr>
<tr>
<td>By default, no IP address is statically bound.</td>
<td></td>
</tr>
</tbody>
</table>
Table 441 Configure to assign IP addresses by static binding

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind an IP address to the MAC address of a DHCP client or a client ID statically</td>
<td>Configure the MAC address to which the IP address is to be statically bound</td>
<td>static-bind mac-address mac-address</td>
</tr>
<tr>
<td></td>
<td>Configure the client ID to which the IP address is to be statically bound</td>
<td>static-bind client-identifier client-identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One of these two options is required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no MAC address or client ID to which an IP address is to be statically bound is configured.</td>
</tr>
</tbody>
</table>

- The static-bind ip-address command and the static-bind mac-address command or the static-bind client-identifier command must be coupled.

- In the same global DHCP address pool, if you configure the static-bind client-identifier command after configuring the static-bind mac-address command, the new configuration overwrites the previous one, and vice versa.

- In the same global DHCP address pool, if the static-bind ip-address command, the static-bind mac-address command, or the static-bind client-identifier is executed repeatedly, the new configuration overwrites the previous one.

- The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise static binding does not take effect.

- A client can permanently use the statically-bound IP address that it has obtained. The IP address is not limited by the lease time of the IP addresses in the address pool.

To improve security and avoid malicious attack to the unused sockets, Switch 5500s provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.

- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After a DHCP address pool is created by executing the dhcp server ip-pool command, the UDP 67 and UDP 68 ports used by DHCP are enabled.

- After a DHCP address pool is deleted by executing the undo dhcp server ip-pool command and all other DHCP functions are disabled, UDP 67 and UDP 68 ports used by DHCP are disabled accordingly.

Configuring the dynamic IP address allocation mode

IP addresses dynamically assigned to DHCP clients (including those that are permanently leased and those that are temporarily leased) belong to addresses segments that are previously specified. Currently, an address pool can contain only one address segment, whose ranges are determined by the subnet mask.

To avoid address conflicts, the DHCP server automatically excludes IP addresses (used by the gateway, FTP server and so forth) specified with the dhcp server forbidden-ip command from dynamic allocation.

The lease time can differ with address pools. But that of the IP addresses of the same address pool are the same. Lease time is not inherited, that is to say, the
lease time of a child address pool is not affected by the configuration of the parent address pool.

### Table 442  Configure to assign IP addresses dynamically

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool pool-name</td>
<td>-</td>
</tr>
<tr>
<td>Set the IP address segment whose IP address are to be assigned dynamically</td>
<td>network network-address [mask mask ]</td>
<td>Required By default, no IP address segment is set. That is, no IP address is available for being assigned.</td>
</tr>
<tr>
<td>Configure the lease time</td>
<td>expired { day day [ hour hour [ minute minute ] ]</td>
<td>Optional The default lease time is one day</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Specify the IP addresses that are not dynamically assigned</td>
<td>dhcp server forbidden-ip low-ip-address [high-ip-address]</td>
<td>Optional By default, except the IP addresses of DHCP server interfaces, all IP addresses in a DHCP address pool are assignable.</td>
</tr>
</tbody>
</table>

- In the same DHCP global address pool, the network command can be executed repeatedly. In this case, the new configuration overwrites the previous one.
- The dhcp server forbidden-ip command can be executed repeatedly. That is, you can configure multiple IP addresses that are not dynamically assigned to DHCP clients.
- If an IP address that is not to be automatically assigned has been configured as a statically-bound IP address, the DHCP server still assigns this IP address to the client whose MAC address or ID has been bound.

### Configuring a Domain Name Suffix for the DHCP Client

You can configure a domain name suffix in each DHCP address pool on the DHCP server. The DHCP server will provide the domain name suffix together with an IP address to the DHCP client.

With this suffix assigned, the client needs only input part of the domain name, and the system will add the domain name suffix for name resolution. For details about DNS, refer to “Configuring Domain Name Resolution” on page 1021.

### Table 443  Configure a domain name suffix for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool pool-name</td>
<td>-</td>
</tr>
<tr>
<td>Configure a domain name suffix for the client</td>
<td>domain-name domain-name</td>
<td>Required Not configured by default.</td>
</tr>
</tbody>
</table>
Configuring DNS Servers for the DHCP Client

If a client accesses a host on the Internet through domain name, DNS (domain name system) is needed to translate the domain name into the corresponding IP address. To enable DHCP clients to access hosts on the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP address pool.

Table 444  Configure DNS servers for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool pool-name</td>
<td></td>
</tr>
<tr>
<td>Configure DNS server addresses for DHCP clients</td>
<td>dns-list ip-address&amp;&lt;1-8&gt;</td>
<td>Required, By default, no DNS server address is configured.</td>
</tr>
</tbody>
</table>

Configuring WINS Servers for the DHCP Client

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by Windows internet naming service (WINS) servers. So you need to perform WINS-related configuration for most Windows-based hosts.

To implement host name-to-IP address translation for DHCP clients, you should enable the DHCP server to assign WINS server addresses when assigning IP addresses to DHCP clients. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- B-node. Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.

- P-node. Nodes of this type establish their mappings by sending unicast packets to WINS servers. (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.

- M-node. Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.

- H-node. Nodes of this type are b-nodes mixed with peer-to-peer features. (The character h stands for the word hybrid), that is to say, this type of nodes obtain mappings by sending unicast packets to WINS servers first. If they fail to obtain mappings, they send broadcast packets to obtain mappings.
CHAPTER 53: DHCP SERVER CONFIGURATION

If b-node is specified for the client, you don’t need to specify any WINS server address.

### Configuring Gateways for the DHCP Client

Gateways are necessary for DHCP clients to access servers/hosts outside the current network segment. After you configure gateway addresses on a DHCP server, the DHCP server provides the gateway addresses to DHCP clients as well while assigning IP addresses to them.

You can configure gateway addresses for address pools on a DHCP server. Currently, you can configure up to eight gateway addresses for a global DHCP address pool.

### Configuring BIMS Server Information for the DHCP Client

A DHCP client performs regular software update and backup using configuration files obtained from a branch intelligent management system (BIMS) server. Therefore, the DHCP server needs to offer DHCP clients the BIMS server IP address, port number, shared key from the DHCP address pool.

### Table 445  Configure WINS servers and NetBIOS node type or the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>pool-name</td>
<td></td>
</tr>
<tr>
<td>Configure WINS server addresses for DHCP clients</td>
<td>nbns-list ip-address&amp;&lt;1-8&gt;</td>
<td>Required By default, no WINS server address is configured.</td>
</tr>
<tr>
<td>Configure DHCP clients to be of a specific NetBIOS node type</td>
<td>netbios-type { b-node</td>
<td>h-node</td>
</tr>
</tbody>
</table>

### Table 446  Configure gateways for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>pool-name</td>
<td></td>
</tr>
<tr>
<td>Configure gateway addresses for DHCP clients</td>
<td>gateway-list ip-address&amp;&lt;1-8&gt;</td>
<td>Required By default, no gateway address is configured.</td>
</tr>
</tbody>
</table>

### Table 447  Configure BIMS server information for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
Configuring the Global Address Pool Based DHCP Server

Configuring Option 184 Parameters for the Client with Voice Service

Option 184 is a reserved option, and the information it carries can be customized. You can define four sub-options for this option after enabling the DHCP server. Thus, besides obtaining an IP address, the DHCP client with voice services can obtain voice related parameters from the DHCP address pool.

Basic concept

The four sub-options of Option 184 mainly carry information about voice. The following lists the sub-options and the carried information:

- Sub-option 1: IP address of the network call processor (NCP-IP).
- Sub-option 2: IP address of the alternate server (AS-IP).
- Sub-option 3: Voice VLAN configuration.
- Sub-option 4: Fail-over call routing.

Meanings of the sub-options for Option 184

<table>
<thead>
<tr>
<th>Sub-option</th>
<th>Feature</th>
<th>Function</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCP-IP (sub-option 1)</td>
<td>The NCP-IP sub-option carries the IP address of the network call processor (NCP).</td>
<td>The IP address of the NCP server carried by sub-option 1 of Option 184 is intended for identifying the server serving as the network call controller and the server used for application downloading.</td>
<td>When used in Option 184, this sub-option must be the first sub-option, that is, sub-option 1</td>
</tr>
<tr>
<td>AS-IP (sub-option 2)</td>
<td>The AS-IP sub-option carries the IP address of the alternate server (AS).</td>
<td>The alternate NCP server identified by sub-option 2 of Option 184 acts as the backup of the NCP server. The NCP server specified by this option is used only when the IP address carried by the NCP-IP sub-option is unreachable or invalid.</td>
<td>The AS-IP sub-option takes effect only when sub-option 1 (that is, the NCP-IP sub-option) is defined</td>
</tr>
</tbody>
</table>

Table 447 Configure BIMS server information for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool pool-name</td>
<td>-</td>
</tr>
<tr>
<td>Configure the BIMS server information to be assigned to the DHCP client</td>
<td>bims-server ip ip-address [ port port-number ] sharekey key</td>
<td>Required By default, no BIMS server information is configured.</td>
</tr>
</tbody>
</table>
CHAPTER 53: DHCP SERVER CONFIGURATION

For the configurations specifying to add sub-option 2, sub-option 3, and sub-option 4 in the response packets to take effect, you need to configure the DHCP server to add sub-option 1.

Mechanism of using Option 184 on DHCP server

The DHCP server encapsulates the information for Option 184 to carry in the response packets sent to the DHCP clients. Supposing that the DHCP clients are on the same segment as the DHCP server, the mechanism of Option 184 on the DHCP server is as follows:

1. A DHCP client sends to the DHCP server a request packet carrying Option 55, which indicates the client requests the configuration parameters of Option 184.

2. The DHCP server checks the request list in Option 55 carried by the request packet, and then adds the sub-options of Option 184 in the Options field of the response packet to be sent to the DHCP client.

### Table 448 Meanings of the sub-options for Option 184

<table>
<thead>
<tr>
<th>Sub-option</th>
<th>Feature</th>
<th>Function</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN Configuration</td>
<td>The voice VLAN configuration sub-option carries the ID of the voice VLAN and the flag indicating whether the voice VLAN identification function is enabled.</td>
<td>The sub-option 3 of Option 184 comprises two parts:</td>
<td></td>
</tr>
<tr>
<td>(sub-option 3)</td>
<td></td>
<td>■ One part carries the flag indicating whether the voice VLAN identification function is enabled.</td>
<td>■ A flag value of 0 indicates that the voice VLAN identification function is not enabled, in which case the information carried by the VLAN ID part will be neglected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ The other part carries the ID of the voice VLAN.</td>
<td>■ A flag value of 1 indicates that the voice VLAN identification function is enabled.</td>
</tr>
<tr>
<td>Fail-Over Call Routing</td>
<td>The fail-over call routing sub-option carries the IP address for fail-over call routing and the associated dial number. The IP address for fail-over call routing and the dial number in sub-option 4 of Option 184 refer to the IP address and dial number of the Session Initiation Protocol (SIP) peer.</td>
<td>When the NCP server is unreachable, a SIP user can use the configured IP address and dial number of the peer to establish a connection and communicate with the peer SIP user.</td>
<td></td>
</tr>
</tbody>
</table>
Only when the DHCP client specifies in Option 55 of the request packet that it requires Option 184, does the DHCP server add Option 184 in the response packet sent to the client.

Configuring Option 184 Parameters for the DHCP Client with Voice Service

Table 449 Configure Option 184 parameters for the DHCP client with voice service

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool</td>
<td></td>
</tr>
<tr>
<td>Specify the IP address of the</td>
<td>voice-config ncp-ip</td>
<td>Required</td>
</tr>
<tr>
<td>primary network calling processor</td>
<td>ip-address</td>
<td>Not specified by default</td>
</tr>
<tr>
<td>Specify the IP address of the</td>
<td>voice-config as-ip</td>
<td>Optional</td>
</tr>
<tr>
<td>backup network calling processor</td>
<td>ip-address</td>
<td>Not specified by default</td>
</tr>
<tr>
<td>Configure the voice VLAN</td>
<td>voice-config voice-vlan</td>
<td>Optional</td>
</tr>
<tr>
<td>Specify the failover IP address</td>
<td>voice-config fail-over</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>ip-address dialer-string</td>
<td>No failover IP address is specified by default</td>
</tr>
</tbody>
</table>

Specify an IP address for the network calling processor before performing other configuration.

Configuring the TFTP Server and Bootfile Name for the DHCP Client

This task is to specify the IP address and name of a TFTP server and the bootfile name in the DHCP global address pool. The DHCP clients use these parameters to contact the TFTP server, requesting the configuration file used for system initialization, which is called auto-configuration. The request process of the client is described below:

1. When a switch starts up without loading any configuration file, the system sets the specified interface (VLAN-interface 1) as the DHCP client to request from the DHCP server parameters such as the IP address and name of a TFTP server, and bootfile name.

2. After getting related parameters, the DHCP client will send a TFTP request to obtain the configuration file from the specified TFTP server for system initialization. If the client cannot get related parameters, it will perform system initialization without loading any configuration file.

To implement auto-configuration, you need to specify the IP address and name of a TFTP server and the bootfile name on the DHCP server, but you do not need to perform any configuration on the DHCP client.

When Option 55 in a client's request contains parameters of Option 66, Option 67, or Option 150, the DHCP server will return the IP address and name of the specified TFTP server, bootfile name and an IP address to the client, which uses such information to complete auto-configuration.
By configuring self-defined DHCP options, you can:

- Define new DHCP options. New configuration options will come out with DHCP development. To support new options, you can add them into the attribute list of the DHCP server.

- Extend existing DHCP options. When the current DHCP options cannot meet customers’ requirements (for example, you cannot use the `dns-list` command to configure more than eight DNS server addresses), you can configure a self-defined option for extension.

### Configuring a Self-Defined DHCP Option

<table>
<thead>
<tr>
<th>Table 450</th>
<th>Configure the TFTP server and bootfile name for the DHCP client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter DHCP address pool view</td>
<td>dhcp server ip-pool pool-name</td>
</tr>
<tr>
<td>Specify the TFTP server</td>
<td>tftp-server ip-address ip-address</td>
</tr>
<tr>
<td>Specify the name of the TFTP server</td>
<td>tftp-server domain-name domain-name</td>
</tr>
<tr>
<td>Specify the bootfile name</td>
<td>bootfile-name bootfile-name</td>
</tr>
</tbody>
</table>

**CAUTION:** Be cautious when configuring self-defined DHCP options because such configuration may affect the DHCP operation process.

### Configuring the Interface Address Pool Based DHCP Server

**CAUTION:** In the interface address pool mode, after the addresses in the interface address pool have been assigned, the DHCP server picks IP addresses from the global interface address pool containing the network segment of the interface address pool and assigns them to the DHCP clients. As a result, the IP addresses obtained from global address pools and those obtained from interface address pools are not on the same network segment, so the clients cannot communicate with each other.
Configuring the Interface Address Pool Based DHCP Server

Therefore, in the interface address pool mode, if the DHCP clients in a VLAN need to obtain IP addresses from the same network segment, the number of DHCP clients cannot exceed the number of the IP addresses assignable in the VLAN interface address pool.

Configuration Task List

An interface address pool is created when the interface is assigned a valid unicast IP address and you execute the dhcp select interface command in interface view. The IP addresses contained in it belong to the network segment where the interface resides in and are available to the interface only.

You can perform certain configurations for DHCP address pools of an interface or multiple interfaces within specified interface ranges. Configuring for multiple interfaces eases configuration work load and makes you to configure in a more convenient way.

Table 452  DHCP server interface address pool configuration task list

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling the Interface Address Pool Mode on Interface(s)” on page 615</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring an Address Allocation Mode for an Interface Address Pool” on page 616</td>
<td>One of the two options is required. And these two options can be configured at the same time.</td>
</tr>
<tr>
<td>“Configuring the static IP address allocation mode” on page 616</td>
<td></td>
</tr>
<tr>
<td>“Configuring the dynamic IP address allocation mode” on page 617</td>
<td></td>
</tr>
<tr>
<td>“Configuring a Domain Name Suffix for the DHCP Client” on page 618</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring DNS Servers for the DHCP Client” on page 619</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring WINS Servers for the DHCP Client” on page 619</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring BIMS Server Information for the DHCP Client” on page 620</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring Option 184 Parameters for the Client with Voice Service” on page 621</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the TFTP Server and Bootfile Name for the DHCP Client” on page 621</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring a Self-Defined DHCP Option” on page 622</td>
<td>Optional</td>
</tr>
</tbody>
</table>

When a Switch 5500 works in the interface address pool mode as a DHCP server, the only gateway address it can assign to a client is the primary IP address of the interface.

Enabling the Interface Address Pool Mode on Interface(s)

If the DHCP server works in the interface address pool mode, it picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.
CHAPTER 53: DHCP SERVER CONFIGURATION

You need to configure an IP address for the interface before enabling the interface address pool mode on it.

To improve security and avoid malicious attack to the unused sockets, Switch 5500s provide the following functions:

- UDP port 67 and UDP port 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP port 67 and UDP port 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After a DHCP interface address pool is created by executing the `dhcp select interface` command, UDP port 67 and UDP v68 ports used by DHCP are enabled.
- After a DHCP interface address pool is deleted by executing the `undo dhcp select interface` command and all other DHCP functions are disabled, UDP port 67 and UDP port 68 ports used by DHCP are disabled accordingly.

### Configuring an Address Allocation Mode for an Interface Address Pool

IP addresses of an interface address pool can be statically bound to DHCP clients or dynamically allocated to DHCP clients.

**Configuring the static IP address allocation mode**

Some DHCP clients, such as WWW servers, need fixed IP addresses. This is achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client applies for an IP address, the DHCP server finds the IP address corresponding to the MAC address of the DHCP client, and then assigns the IP address to the DHCP client.

When some DHCP clients send DHCP-DISCOVER packets to the DHCP server to apply for IP addresses, they construct client IDs and add them in the DHCP-DISCOVER packets. The DHCP server finds the corresponding IP addresses based on the client IDs and assigns them to the DHCP clients.

<table>
<thead>
<tr>
<th>Table 453</th>
<th>Configure interface address pool mode on interface(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Configure interface address pool mode</td>
<td>On the current interface <code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>dhcp select interface</td>
<td>quit</td>
</tr>
<tr>
<td>On multiple interfaces in system view</td>
<td>`dhcp select interface interface-type interface-number [ to interface-type interface-number</td>
</tr>
</tbody>
</table>

**Table 454** Configure to assign IP addresses by static binding

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
</tbody>
</table>
Configuring the Interface Address Pool Based DHCP Server

The IP addresses statically bound in interface address pools and the interface IP addresses must be in the same network segment.

There is no limit to the number of IP addresses statically bound in an interface address pool, but the IP addresses statically bound in interface address pools and the interface IP addresses must be in the same segment.

An IP address can be statically bound to only one MAC address or one client ID. A MAC address or client ID can be bound with only one IP address statically.

The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise the static binding does not take effect.

Configuring the dynamic IP address allocation mode

As an interface-based address pool is created after the interface is assigned a valid unicast IP address, the IP addresses contained in the address pool belong to the network segment where the interface resides in and are available to the interface only. So specifying the range of the IP addresses to be dynamically assigned is unnecessary.

To avoid address conflicts, the DHCP server automatically excludes IP addresses (used by the gateway, FTP server and so forth) specified with the `dhcp server forbidden-ip` command from dynamic allocation.

To avoid IP address conflicts, the IP addresses to be dynamically assigned to DHCP clients are those not occupied by specific network devices (such as gateways and FTP servers).

The lease time can differ with address pools. But that of the IP addresses of the same address pool are the same. Lease time is not inherited, that is to say, the lease time of a child address pool is not affected by the configuration of the parent address pool.

### Table 454 Configure to assign IP addresses by static binding

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure static binding</td>
<td><code>dhcp server static-bind</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>`ip-address ip-address { client-identifier</td>
<td>By default, static binding is not configured</td>
</tr>
<tr>
<td></td>
<td>mac-address mac-address }</td>
<td></td>
</tr>
</tbody>
</table>

### Table 455 Configure to assign IP addresses dynamically

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
</tbody>
</table>
The dhcp server forbidden-ip command can be executed repeatedly. That is, you can configure multiple IP addresses that are not dynamically assigned to DHCP clients.

Use the dhcp server forbidden-ip command to configure the IP addresses that are not assigned dynamically in global address pools and interface address pools.

If an IP address that is not to be automatically assigned has been configured as a statically-bound IP address, the DHCP server still assigns this IP address to the client whose MAC address or client ID has been bound.

### Configuring a Domain Name Suffix for the DHCP Client

You can configure a suffix for the domain name in each DHCP interface address pool on the DHCP server. The DHCP server provides the domain name suffix together with an IP address for a requesting DHCP client.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a domain name suffix for the clients</td>
<td>In the current interface address pool: interface interface-type interface-number dhcp server expired { day day [ hour hour ] [ minute minute ]</td>
<td>unlimited } quit dhcp server forbidden-ip low-ip-address [ high-ip-address ]</td>
</tr>
<tr>
<td></td>
<td>In multiple interface address pools in system view: dhcp server domain-name domain-name</td>
<td>Not configured by default</td>
</tr>
</tbody>
</table>
Configuring DNS Servers for the DHCP Client

If a client accesses a host on the Internet through domain name, DNS is needed to translate the domain name into the corresponding IP address. To enable DHCP clients to access hosts on the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP interface address pool.

### Table 457 Configure DNS servers for the DHCP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure DNS server addresses for DHCP clients</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the current interface</td>
<td>dhcp server dns-list ip-address&amp;&lt;1-8&gt;</td>
<td>By default, no DNS server address is configured.</td>
</tr>
<tr>
<td></td>
<td>quit</td>
<td></td>
</tr>
</tbody>
</table>
| Configure multiple interfaces in system view | dhcp server dns-list ip-address&<1-8> { interface interface-type interface-number [ to interface-type interface-number ] | all | }

Configuring WINS Servers for the DHCP Client

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by WINS servers. So you need to perform WINS-related configuration for most Windows-based hosts.

To implement host name-to-IP address translation for DHCP clients, you should enable the DHCP server to assign WINS server addresses when assigning IP addresses to DHCP clients. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through the NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- **B-node.** Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.

- **P-node.** Nodes of this type establish their mappings by communicating with WINS servers (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.

- **M-node.** Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.

- **H-node.** Nodes of this type are b-nodes mixed with peer-to-peer features (The character h stands for the word hybrid), that is to say, this type of nodes obtain
mappings by sending unicast packets to WINS servers first. If they fail to obtain mappings, they send broadcast packets to obtain mappings.

**Table 458  Configure WINS servers and NETBIOS node type for the DHCP client**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure WINS server addresses for DHCP clients</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>dhcp server nbns-list ip-address&amp;&lt;1-8&gt; quit</td>
<td>By default, no WINS server address is configured.</td>
</tr>
<tr>
<td>Configure multiple interfaces in system view</td>
<td>dhcp server nbns-list ip-address&amp;&lt;1-8&gt; { interface interface-type interface-number [ to interface-type interface-number ]</td>
<td>all }</td>
</tr>
<tr>
<td>Configure a NetBIOS node type for DHCP clients</td>
<td>interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>dhcp server netbios-type { b-node</td>
<td>h-node</td>
</tr>
<tr>
<td>Configure multiple interfaces in system view</td>
<td>dhcp server netbios-type { b-node</td>
<td>h-node</td>
</tr>
</tbody>
</table>

**Table 459  Configure BIMS server information for the DHCP client**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the BIMS server information to be assigned to the DHCP client</td>
<td>dhcp server bims-server ip ip-address [ port port-number ] sharekey key { interface interface-type interface-number [ to interface-type interface-number ]</td>
<td>all }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no BIMS server information is configured.</td>
</tr>
</tbody>
</table>

If b-node is specified for the client, you don’t need to specify any WINS server address.

**Configuring BIMS Server Information for the DHCP Client**

A DHCP client performs regular software update and backup using configuration files obtained from a branch intelligent management system (BIMS) server. Therefore, the DHCP server needs to offer DHCP clients the BIMS server IP address, port number, shared key from the DHCP address pool.

If b-node is specified for the client, you don’t need to specify any WINS server address.
Configuring Option 184 Parameters for the Client with Voice Service

For details about Option 184, refer to “Configuring Option 184 Parameters for the Client with Voice Service” on page 611.

Table 460 Configure Option 184 parameters for the client with voice service

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure Option 184 in the current interface address pool</td>
<td>Enter interface view interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Specify the primary network calling processor</td>
<td>dhcp server voice-config ncp-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td>Specify the backup network calling processor</td>
<td>dhcp server voice-config as-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the voice VLAN</td>
<td>dhcp server voice-config voice-vlan vlan-id { disable</td>
<td>enable }</td>
</tr>
<tr>
<td>Specify the failover IP address</td>
<td>dhcp server voice-config fail-over ip-address dialer-string</td>
<td>Optional</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Configure Option 184 in multiple interface address pools</td>
<td>Specify the primary network calling processor</td>
<td>dhcp server voice-config ncp-ip ip-address { all</td>
</tr>
<tr>
<td>Specify the backup network calling processor</td>
<td>dhcp server voice-config as-ip ip-address { all</td>
<td>interface-type interface-number [ to interface-type interface-number ] }</td>
</tr>
<tr>
<td>Configure the voice VLAN</td>
<td>dhcp server voice-config voice-vlan vlan-id { disable</td>
<td>enable } { all</td>
</tr>
<tr>
<td>Specify the failover IP address</td>
<td>dhcp server voice-config fail-over ip-address dialer-string { all</td>
<td>interface-type interface-number [ to interface-type interface-number ] }</td>
</tr>
</tbody>
</table>

Specify an IP address for the network calling processor before performing other configuration.

Configuring the TFTP Server and Bootfile Name for the DHCP Client

For related principles, refer to “Configuring the TFTP Server and Bootfile Name for the DHCP Client” on page 613.
Configuring a Self-Defined DHCP Option

By configuring self-defined DHCP options, you can:

- Define new DHCP options. New configuration options will come out with DHCP development. To support new options, you can add them into the attribute list of the DHCP server.

- Extend existing DHCP options. When the current DHCP options cannot meet customers' requirements (for example, you cannot use the dns-list command to configure more than eight DNS server addresses), you can configure a self defined option for extension.

Table 462  Customize DHCP service

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Specify the IP address and name of the TFTP server and the bootfile name in the current interface address pool</td>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Specify the TFTP server</td>
<td>dhcp server tftp-server ip-address ip-address</td>
<td>Optional Not specified by default</td>
</tr>
<tr>
<td>Specify the TFTP server name</td>
<td>dhcp server tftp-server domain-name domain-name</td>
<td></td>
</tr>
<tr>
<td>Specify the bootfile name</td>
<td>dhcp server bootfile-name bootfile-name</td>
<td></td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>Specify the IP address and name of the TFTP server and the bootfile name in the specified interface address pool</td>
<td>Specify the TFTP server</td>
<td>dhcp server tftp-server ip-address ip-address { all</td>
</tr>
<tr>
<td>Specify the TFTP server name</td>
<td>dhcp server tftp-server domain-name domain-name { all</td>
<td>interface interface-type interface-number }</td>
</tr>
<tr>
<td>Specify the bootfile name</td>
<td>dhcp server bootfile-name bootfile-name { all</td>
<td>interface interface-type interface-number }</td>
</tr>
</tbody>
</table>
Configuring DHCP Server Security Functions

DHCP security configuration is needed to ensure the security of DHCP service.

**Prerequisites**
Before configuring DHCP security, you should first complete the DHCP server configuration (either global address pool-based or interface address pool-based DHCP server configuration).

**Enabling Unauthorized DHCP Server Detection**
If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the client.

With this feature enabled, when receiving a DHCP message with the siaddr field not being 0 from a client, the DHCP server will record the value of the siaddr field and the receiving interface. The administrator can use such information to check out any DHCP unauthorized servers.

<table>
<thead>
<tr>
<th>Table 462</th>
<th>Customize DHCP service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Configure customized options</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>Configure the current interface</td>
<td>dhcp server option code { ascii ascii-string</td>
</tr>
<tr>
<td></td>
<td>hex hex-string&amp;&lt;1-10&gt;</td>
</tr>
<tr>
<td></td>
<td>ip-address ip-address&amp;&lt;1-8&gt; }</td>
</tr>
<tr>
<td></td>
<td>quit</td>
</tr>
<tr>
<td></td>
<td>dhcp server option code { ascii ascii-string</td>
</tr>
<tr>
<td></td>
<td>hex hex-string&amp;&lt;1-10&gt;</td>
</tr>
<tr>
<td></td>
<td>ip-address ip-address&amp;&lt;1-8&gt; }</td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td>all</td>
</tr>
</tbody>
</table>

**CAUTION:** Be cautious when configuring self-defined DHCP options because such configuration may affect the DHCP operation process.

<table>
<thead>
<tr>
<th>Table 463</th>
<th>Enable unauthorized DHCP server detection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enable the unauthorized DHCP server detecting function</td>
<td>dhcp server detect</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once. The administrator needs to find unauthorized DHCP servers from the system log information.

Configuring IP Address Detecting

To avoid IP address conflicts caused by assigning the same IP address to multiple DHCP clients simultaneously, you can configure a DHCP server to detect an IP address before it assigns the address to a DHCP client.

The DHCP server pings the IP address to be assigned using ICMP. If the server gets a response within the specified period, the server will ping another IP address; otherwise, the server will ping the IP addresses once again until the specified number of ping packets are sent. If still no response, the server will assign the IP address to the requesting client (The DHCP client probes the IP address by sending gratuitous ARP packets).

### Table 464  Configure IP address detecting

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of ping operations performed by a DHCP server</td>
<td>dhcp server ping packets number</td>
<td>Optional By default, a DHCP server performs the ping operation twice to test an IP address.</td>
</tr>
<tr>
<td>Set the response timeout time of each ping operation</td>
<td>dhcp server ping timeout milliseconds</td>
<td>Optional The default timeout time is 500 milliseconds.</td>
</tr>
</tbody>
</table>

Configuring DHCP Accounting Functions

**Introduction to DHCP Accounting**

DHCP accounting allows a DHCP server to notify the RADIUS server of the start/end of accounting when it assigns/releases a lease. The cooperation of DHCP server and RADIUS server implements the network accounting function and ensures network security at the same time.

**DHCP Accounting Fundamentals**

After you complete AAA and RADIUS configuration on a switch with the DHCP server function enabled, the DHCP server acts as a RADIUS client. For the authentication process of the DHCP server acting as a RADIUS client, refer to “AAA Configuration” on page 519. The following describes only the accounting interaction between DHCP server and RADIUS server.

- After sending a DHCP-ACK packet with the IP configuration parameters to the DHCP client, the DHCP server sends an Accounting START packet to a specified RADIUS server. The RADIUS server processes the packet, makes a record, and sends a response to the DHCP server.
- Once releasing a lease, the DHCP server sends an Accounting STOP packet to the RADIUS server. The RADIUS server processes the packet, stops the recording for the DHCP client, and sends a response to the DHCP server. A lease can be released for the reasons such as lease expiration, a release request.
DHCP Accounting Configuration

Prerequisites
Before configuring DHCP accounting, make sure that:
- The DHCP server is configured and operates properly. Address pools and lease time are configured.
- DHCP clients are configured and DHCP service is enabled.
- The network operates properly.

Configuring DHCP Accounting

Table 465  Configure DHCP accounting

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter address pool view</td>
<td>dhcp server ip-pool</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>pool-name</td>
<td></td>
</tr>
<tr>
<td>Enable DHCP accounting</td>
<td>accounting domain</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>domain-name</td>
<td>The domain identified by the domain-name argument can be created by using the domain command.</td>
</tr>
</tbody>
</table>

Enabling the DHCP Server to Process Option 82

If a DHCP server is enabled to process Option 82, after the DHCP server receives packets containing Option 82, the DHCP server adds Option 82 into the responses when assigning IP addresses and other configuration information to the clients.

If a DHCP server is configured to ignore Option 82, after the DHCP server receives packets containing Option 82, the DHCP server will not add Option 82 into the responses when assigning IP addresses and other configuration information to the clients.

For details of Option 82, see “Option 82 Support on DHCP Relay Agent” on page 634.

Table 466  Configure the DHCP server to process Option 82

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the DHCP server to process Option 82</td>
<td>dhcp server relay information enable</td>
<td>Optional By default, the DHCP server supports Option 82.</td>
</tr>
</tbody>
</table>
Displaying and Maintaining the DHCP Server

You can verify your DHCP-related configuration by executing the `display` command in any view.

To clear the information about DHCP servers, execute the `reset` command in user view.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the statistics on IP address conflicts</td>
<td><code>display dhcp server conflict</code> (all</td>
<td>ip ip-address)</td>
</tr>
<tr>
<td>Display lease expiration information</td>
<td><code>display dhcp server expired</code> (ip ip-address</td>
<td>pool [pool-name]</td>
</tr>
<tr>
<td>Display the free IP addresses</td>
<td><code>display dhcp server free-ip</code></td>
<td></td>
</tr>
<tr>
<td>Display information about address binding</td>
<td><code>display dhcp server ip-in-use</code> (ip ip-address</td>
<td>pool [pool-name]</td>
</tr>
<tr>
<td>Display the statistics on a DHCP server</td>
<td><code>display dhcp server statistics</code></td>
<td></td>
</tr>
<tr>
<td>Display information about DHCP address pool tree</td>
<td><code>display dhcp server tree</code> (pool [pool-name]</td>
<td>interface</td>
</tr>
<tr>
<td>Clear IP address conflict statistics</td>
<td><code>reset dhcp server conflict</code> (all</td>
<td>ip ip-address)</td>
</tr>
<tr>
<td>Clear dynamic address binding information</td>
<td><code>reset dhcp server ip-in-use</code> (ip ip-address</td>
<td>pool [pool-name]</td>
</tr>
<tr>
<td>Clear the statistics on a DHCP server</td>
<td><code>reset dhcp server statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

Executing the `save` command will not save the lease information on a DHCP server to the flash memory. Therefore, the configuration file contains no lease information after the DHCP server restarts or you clear the lease information by executing the `reset dhcp server ip-in-use` command. In this case, any lease-update requests will be denied, and the clients must apply for IP addresses again.

DHCP Server Configuration Examples

Currently, DHCP networking can be implemented in two ways. One is to deploy the DHCP server and DHCP clients in the same network segment. This enables the clients to communicate with the server directly. The other is to deploy the DHCP server and DHCP clients in different network segments. In this case, IP address assigning is carried out through DHCP relay agent. Note that DHCP server configuration is the same in both scenarios.
Network requirements

- The DHCP server (Switch A) assigns IP address to clients in subnet 10.1.1.0/24, which is subnetted into 10.1.1.0/25 and 10.1.1.128/25.
- The IP addresses of VLAN interfaces 1 and 2 on Switch A are 10.1.1.1/25 and 10.1.1.129/25 respectively.
- In the address pool 10.1.1.0/25, the address lease duration is ten days and twelve hours, domain name suffix aabbcc.com, DNS server address 10.1.1.2, gateway 10.1.1.126, and WINS server 10.1.1.4.
- In the address pool 10.1.1.128/25, the address lease duration is five days, domain name suffix aabbcc.com, DNS server address 10.1.1.2, and gateway address 10.1.1.254, and there is no WINS server address.

*If you use the inheriting relation of parent and child address pools, make sure that the number of the assigned IP addresses does not exceed the number of the IP addresses in the child address pool; otherwise extra IP addresses will be obtained from the parent address pool, and the attributes (for example, gateway) also are based on the configuration of the parent address pool.*

For example, in the network to which VLAN-interface 1 is connected, if multiple clients apply for IP addresses, the child address pool 10.1.1.0/25 assigns IP addresses first. When the IP addresses in the child address pool have been assigned, if other clients need IP addresses, the IP addresses will be assigned from the parent address pool 10.1.1.0/24 and the attributes will be based on the configuration of the parent address pool.

For this example, the number of clients applying for IP addresses from VLAN-interface 1 is recommended to be less than or equal to 122 and the number of clients applying for IP addresses from VLAN-interface 2 is recommended to be less than or equal to 124.

Network diagram

**Figure 177** Network diagram for DHCP configuration

**Configuration procedure**

1. Configure a VLAN and add a port in this VLAN, and then configure the IP address of the VLAN interface (omitted).
2. Configure DHCP service.
# Enable DHCP.

```plaintext
<SwitchA> system-view
[SwitchA] dhcp enable
```

# Configure the IP addresses that are not dynamically assigned. (That is, the IP addresses of the DNS server, WINS server, and gateways.)

```plaintext
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

# Configure DHCP address pool 0, including address range, domain name suffix of the clients, and domain name server address.

```plaintext
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] domain-name aabbcc.com
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] quit
```

# Configure DHCP address pool 1, including address range, gateway, WINS server address and lease time.

```plaintext
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] expired day 10 hour 12
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

# Configure DHCP address pool 2, including address range, gateway and lease time.

```plaintext
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
```

**DHCP Server with Option 184 Support Configuration Example**

**Network requirements**

A 3COM VCX device operating as a DHCP client requests the DHCP server for all sub-options of Option 184. A Switch 5500 operates as the DHCP server. The Option 184 support function is configured for a global DHCP address pool. The sub-options of Option 184 are as follows:

- NCP-IP: 3.3.3.3
- AS-IP: 2.2.2.2
- Voice VLAN configuration: voice VLAN: enabled; voice VLAN ID: 3
- Fail-over routing: IP address: 1.1.1.1; dialer string: 99*
Network diagram

**Figure 178** Network diagram for Option 184 support configuration

![Network diagram]

**Configuration procedure**

1. Configure the DHCP client.
   
   Configure the 3COM VCX device to operate as a DHCP client and to request for all sub-options of Option 184. (Configuration process omitted)

2. Configure the DHCP server.
   
   # Enter system view.

   ```
   <5500> system-view
   
   # Add Ethernet 1/0/1 to VLAN 2 and configure the IP address of VLAN 2 interface to be 10.1.1.1/24.
   
   [5500] vlan 2
   [5500-vlan2] port Ethernet 1/0/1
   [5500-vlan2] quit
   [5500] interface Vlan-interface 2
   [5500-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
   [5500-Vlan-interface2] quit
   
   # Configure VLAN-interface 2 to operate in the DHCP server mode.
   
   [5500] dhcp select global interface Vlan-interface 2
   
   # Enter DHCP address pool view.
   
   [5500] dhcp server ip-pool 123
   
   # Configure sub-options of Option 184 in global DHCP address pool view.
   
   [5500-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
   [5500-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
   [5500-dhcp-pool-123] voice-config as-ip 2.2.2.2
   [5500-dhcp-pool-123] voice-config voice-vlan 3 enable
   [5500-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
DHCP Accounting
Configuration Example

Network requirements
- The DHCP server connects to a DHCP client and a RADIUS server respectively through Ethernet 1/0/1 and Ethernet 1/0/2.
- Ethernet 1/0/1 belongs to VLAN 2; Ethernet 1/0/2 belongs to VLAN 3.
- The IP address of VLAN-interface 1 is 10.1.1.1/24, and that of VLAN-interface 2 is 10.1.2.1/24.
- The IP address of the RADIUS server is 10.1.2.2/24.
- DHCP accounting is enabled on the DHCP server.
- The IP addresses of the global DHCP address pool belongs to the network segment 10.1.1.0. The DHCP server operates as a RADIUS client and adopts AAA for authentication.

Network diagram

Figure 179  Network diagram for DHCP accounting configuration

![Network diagram](image)

Configuration procedure

# Enter system view.

<5500> system-view

# Create VLAN 2.

[5500] vlan 2
[5500-vlan2] quit

# Create VLAN 3.

[5500] vlan 3
[5500-vlan3] quit

# Enter Ethernet 1/0/1 port view and add the port to VLAN 2.

[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] port access vlan 2
[5500-Ethernet1/0/1] quit

# Enter Ethernet 1/0/2 port view and add the port to VLAN 3.

[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port access vlan 2
[5500-Ethernet1/0/2] quit

# Enter VLAN 2 interface view and assign the IP address 10.1.1.1/24 to the VLAN interface.
Troubleshooting a DHCP Server

Symptom
The IP address dynamically assigned by a DHCP server to a client conflicts with the IP address of another host.

Analysis
With DHCP enabled, IP address conflicts are usually caused by IP addresses that are manually configured on hosts.

Solution
- Disconnect the DHCP client from the network and then check whether there is a host using the conflicting IP address by performing ping operation on another host on the network, with the conflicting IP address as the destination and an enough timeout time.
- The IP address is manually configured on a host if you receive a response packet of the ping operation. You can then disable the IP address from being dynamically assigned by using the dhcp server forbidden-ip command on the DHCP server.
- Attach the DHCP client to the network, release the dynamically assigned IP address and obtain an IP address again. For example, enter DOS by executing the cmd command in Windows XP, and then release the IP address by executing the ipconfig/release command. Then obtain an IP address again by executing the ipconfig/renew command.
Currently, the interface-related DHCP relay agent configurations can only be made on VLAN interfaces.

Introduction to DHCP Relay Agent

Usage of DHCP Relay Agent

Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP relay agent is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

DHCP Relay Agent Fundamentals

Figure 180 illustrates a typical DHCP relay agent application.

Figure 180  Typical DHCP relay agent application

In the process of dynamic IP address assignment through the DHCP relay agent, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay agent. The following sections only describe the
forwarding process of the DHCP relay agent. For the interaction process of the packets, see “Obtaining IP Addresses Dynamically” on page 598.

1. After receiving the DHCP-DISCOVER or DHCP-REQUEST broadcast from the client, the network device providing the DHCP relay agent function unicasts the message to the designated DHCP server based on the configuration.

2. The DHCP server selects an IP address and other parameters and sends the configuration information to the DHCP relay agent that relays the information to the client (the sending mode is decided by the flag filed in the client’s DHCP-DISCOVER packet, refer to “DHCP Packet Format” on page 599 for details).

Option 82 Support on DHCP Relay Agent

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. With this option, 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. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content of Option 82

Option 82 has no unified definition in RFC 3046. Its padding information varies with vendors. Currently, Switch 5500 Family that operate as DHCP relay agents support the extended padding format of Option 82 sub-options. By default, the sub-options of Option 82 are padded as follows, as shown in Figure 181 and Figure 182. (The content in brackets is the fixed value of each field.)

- sub-option 1: Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client’s request.
- sub-option 2: Padded with the bridge MAC address of the DHCP relay agent device that received the client’s request.

Figure 181 Padding contents for sub-option 1 of Option 82

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>15</td>
<td>23</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>Sub-option Type (0x01)</td>
<td>Length (0x06)</td>
<td>Circuit ID Type (0x00)</td>
<td>Circuit ID Length (0x04)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td></td>
<td>Port Index</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 182 Padding contents for sub-option 2 of Option 82

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>15</td>
<td>23</td>
<td>31</td>
</tr>
<tr>
<td>Sub-option Type (0x02)</td>
<td>Length (0x08)</td>
<td>Remote ID Type (0x00)</td>
<td>Remote ID Length (0x06)</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mechanism of Option 82 supported on DHCP relay agent

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay agent is similar to that for the client to obtain an IP address...
from a DHCP server directly. The following are the mechanism of Option 82 support on DHCP relay agent.

1 Upon receiving a DHCP request, the DHCP relay agent checks whether the packet contains Option 82 and processes the packet accordingly.
   - If the request packet contains Option 82, the DHCP relay agent processes the packet depending on the configured strategy (that is, discards the packet, replaces the original Option 82 in the packet with its own, or leaves the original Option 82 unchanged in the packet), and forwards the packet (if not discarded) to the DHCP server.
   - If the request packet does not contain Option 82, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server.

2 Upon receiving the packet returned from the DHCP server, the DHCP relay agent strips Option 82 from the packet and forwards the packet with the DHCP configuration information to the DHCP client.

Request packets sent by a DHCP client fall into two categories: DHCP-DISCOVER packets and DHCP-REQUEST packets. As DHCP servers coming from different manufacturers process DHCP request packets in different ways (that is, some DHCP servers process Option 82 in DHCP-DISCOVER packets, whereas the rest process Option 82 in DHCP-REQUEST packets), a DHCP relay agent adds Option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

### Configuring the DHCP Relay Agent

If a switch belongs to an IRF fabric, you need to enable the UDP-helper function on it before configuring it as a DHCP relay agent.

### Configuration Task List

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Enabling DHCP&quot; on page 635</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Correlating a DHCP Server Group with a Relay Agent Interface&quot; on page 636</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring DHCP Relay Agent Security Functions&quot; on page 636</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the DHCP Relay Agent to Support Option 82&quot; on page 638</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Enabling DHCP

Make sure to enable DHCP before you perform other DHCP relay-related configurations, since other DHCP-related configurations cannot take effect with DHCP disabled.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>dhcp enable</td>
<td>Required By default, DHCP is enabled</td>
</tr>
</tbody>
</table>
Correlating a DHCP Server Group with a Relay Agent Interface

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When an interface of the relay agent establishes a correlation with the DHCP server group, the interface will forward received DHCP packets to all servers in the server group.

Table 470  Correlate a DHCP server group with a relay agent interface

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the DHCP server IP address(es) in a specified DHCP server group</td>
<td>dhcp-server groupNo ip</td>
<td>Required By default, no DHCP server IP address is configured in a DHCP server group.</td>
</tr>
<tr>
<td></td>
<td>ip-address&amp;&lt;1-8&gt;</td>
<td></td>
</tr>
<tr>
<td>Map an interface to a DHCP server group</td>
<td>interface interface-type</td>
<td>Required By default, a VLAN interface is not mapped to any DHCP server group.</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dhcp-server groupNo</td>
<td></td>
</tr>
</tbody>
</table>

To improve security and avoid malicious attack to the unused SOCKETS, Switch 5500s provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- When a VLAN interface is mapped to a DHCP server group with the dhcp-server command, the DHCP relay agent is enabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are enabled.
- When the mapping between a VLAN interface and a DHCP server group is removed with the undo dhcp-server command, DHCP services are disabled. At the same time, UDP 67 and UDP 68 ports are disabled.

- You can configure up to eight DHCP server IP addresses in a DHCP server group.
- You can map multiple VLAN interfaces to one DHCP server group. But one VLAN interface can be mapped to only one DHCP server group.
- If you execute the dhcp-server groupNo command repeatedly, the new configuration overwrites the previous one.
- You need to configure the group number specified in the dhcp-server groupNo command in VLAN interface view by using the command dhcp-server groupNo ip ip-address&<1-8> in advance.

Configuring DHCP Relay Agent Security Functions

Configuring address checking

After relaying an IP address from the DHCP server to a DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. 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.

The purpose of the address checking function on DHCP relay agent is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay agent inhibits a user from accessing external networks if the IP address configured on the user end and the MAC address of the user end do not match any entries (including the entries dynamically tracked by the DHCP relay agent and the manually configured static entries) in the user address table on the DHCP relay agent.

Table 471  Configure address checking

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Create a static DHCP user address entry manually</td>
<td>dhcp-security static ip-address mac-address</td>
<td>Optional By default, no static DHCP user address entry is configured.</td>
</tr>
<tr>
<td>Enter interface view</td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Enable the address checking function</td>
<td>address-check enable</td>
<td>Required By default, the address checking function is disabled.</td>
</tr>
</tbody>
</table>

- The **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 (such as the command to enable DHCP) are used.

- Before executing the **address-check enable** command on the interface connected to the DHCP server, you need to configure the static binding of the IP address to the MAC address of the DHCP server. Otherwise, the DHCP client will fail to obtain an IP address.

### Configuring the dynamic client address entry updating function

After relaying an IP address from the DHCP server to the DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. But as a DHCP relay agent does not process DHCP-RELEASE packets, which are sent to DHCP servers by DHCP clients through unicast when the DHCP clients release IP addresses, the user address entries maintained by the DHCP cannot be updated in time. You can solve this problem by enabling the DHCP relay agent handshake function and configuring the dynamic client address entry updating interval.

After the handshake function is enabled, the DHCP relay agent sends the handshake packet (the DHCP-REQUEST packet) periodically to the DHCP server using a client's IP address and its own MAC address.

- If the DHCP relay agent receives the DHCP-ACK packet from the DHCP server, or receives no response from the server within a specified period, the IP address can be assigned. The DHCP relay agent ages out the corresponding entry in the client address table.
If the DHCP relay agent receives the DHCP-NAK packet from the DHCP server, the lease of the IP address does not expire. The DHCP relay agent does not age out the corresponding entry.

Currently, the DHCP relay agent handshake function on a Switch 5500 can only operate with a Windows 2000 DHCP server.

Enabling unauthorized DHCP server detection

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the DHCP client.

With this feature enabled, upon receiving a DHCP message with the siaddr field (IP addresses of the servers offering IP addresses to the client) not being 0 from a client, the DHCP relay agent will record the value of the siaddr field and the receiving interface. The administrator can use this information to check out any DHCP unauthorized servers.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the DHCP relay agent handshake function</td>
<td>dhcp relay hand enable</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enabled by default.</td>
</tr>
<tr>
<td>Set the interval at which the DHCP relay agent dynamically updates the client address entries</td>
<td>dhcp-security tracker { interval</td>
<td>auto }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, auto is adopted, that is, the interval is automatically calculated.</td>
</tr>
</tbody>
</table>

Table 472  Configure the dynamic user address entry updating function

With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once until such information is removed and is recorded again. The administrator needs to find unauthorized DHCP servers from the system log information.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable unauthorized DHCP server detection</td>
<td>dhcp-server detect</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

Table 473  Enable unauthorized DHCP server detection

Prerequisites

Before configuring Option 82 support on a DHCP relay agent, you need to:

- Configure network parameters and relay function of the DHCP relay device.
- Perform assignment strategy-related configurations, such as network parameters of the DHCP server, address pool, and lease time.
- The routes between the DHCP relay agent and the DHCP server are reachable.
Enabling Option 82 support on a DHCP relay agent

The following operations need to be performed on a DHCP relay agent.

Table 474: Enable Option 82 support on a DHCP relay agent

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable Option 82 support on the DHCP relay agent</td>
<td>dhcp relay information enable</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the strategy for the DHCP relay agent to</td>
<td>dhcp relay information strategy</td>
<td>Optional</td>
</tr>
<tr>
<td>process request packets containing Option 82</td>
<td>{ drop</td>
<td>keep</td>
</tr>
</tbody>
</table>

- By default, with the Option 82 support function enabled on the DHCP relay agent, the DHCP relay agent will adopt the replace strategy to process the request packets containing Option 82. However, if other strategies are configured before, then enabling the 82 support on the DHCP relay agent will not change the configured strategies.

- To enable Option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay agent.

Displaying and Maintaining DHCP Relay Agent Configuration

After the preceding configurations, you can execute the `display` command in any view to verify the configurations. You can also execute the `reset` command to clear the statistics information about the specified DHCP server group.

Table 475: Display and maintain DHCP relay agent configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about a specified DHCP server group</td>
<td>display dhcp-server groupNo</td>
<td>The <code>display</code> command can be executed in any view</td>
</tr>
<tr>
<td>Display the information about the DHCP server group to which a specified VLAN interface is mapped</td>
<td>display dhcp-server interface Vlan-interface vlan-id</td>
<td></td>
</tr>
<tr>
<td>Display the specified client address entries on the DHCP relay agent</td>
<td>display dhcp-security [ ip-address</td>
<td>dynamic</td>
</tr>
<tr>
<td>Clear the statistics information of the specified DHCP server group</td>
<td>reset dhcp-server groupNo</td>
<td>The <code>reset</code> command must be executed in user view</td>
</tr>
</tbody>
</table>

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 the figure below, Switch A forwards messages between DHCP clients and the DHCP server to assign IP addresses in subnet 10.10.1.0/24 to the clients.
**CHAPTER 54: DHCP RELAY AGENT CONFIGURATION**

**Network diagram**

**Figure 183** Network diagram for DHCP relay agent

```
DHCP client  DHCP client
      |         |
      Vlan-int1 10.10.1.1/24
      |         |
      Vlan-int2 10.1.1.1/24
      |         |
Switch A DHCP relay
      |         |
      Vlan-int2 10.1.1.1/24
      |         |
Switch B DHCP server

DHCP client  DHCP client
```

**Configuration procedure**

# Enter system view.

```bash
<SwitchA> system-view
```

# Create DHCP server group 1 and configure an IP address of 10.1.1.1 for it.

```bash
[SwitchA] dhcp-server 1 ip 10.1.1.1
```

# Map VLAN interface 1 to DHCP server group 1.

```bash
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] dhcp-server 1
```

- You need to perform corresponding configurations on the DHCP server to enable the DHCP clients to obtain IP addresses from the DHCP server. The DHCP server configurations vary with different DHCP server devices, so the configurations are omitted.
- The DHCP relay agent and server must be able to communicate with each other.

---

**Troubleshooting DHCP Relay Agent Configuration**

**Symptom**

A client fails to obtain configuration information through a DHCP relay agent.

**Analysis**

This problem may be caused by improper DHCP relay agent configuration. When a DHCP relay agent operates improperly, you can locate the problem by enabling debugging and checking the information about debugging and interface state (You can display the information by executing the corresponding display command.)

**Solution**

- Check if DHCP is enabled on the DHCP server and the DHCP relay agent.
■ Check if an address pool that is on the same network segment with the DHCP clients is configured on the DHCP server.

■ Check if a reachable route is configured between the DHCP relay agent and the DHCP server.

■ Check the DHCP relay agent. Check if the correct DHCP server group is configured on the interface connecting the network segment where the DHCP client resides. Check if the IP address of the DHCP server group is correct.

■ If the `address-check enable` command is configured on the interface connected to the DHCP server, verify the DHCP server’s IP-to-MAC address binding entry is configured on the DHCP relay agent; otherwise the DHCP client cannot obtain an IP address.
DHCP Snooping Configuration

Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

- Switches can track DHCP clients’ IP addresses through the security function of the DHCP relay agent operating at the network layer.
- Switches can track DHCP clients’ IP addresses through the DHCP snooping function at the data link layer.

When an unauthorized DHCP server exists in the network, a DHCP client may obtain an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Figure 184 illustrates a typical network diagram for DHCP snooping application, where Switch A is a Switch 5500.

Figure 184  Typical network diagram for DHCP snooping application
DHCP snooping listens to the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

- DHCP-REQUEST packet
- DHCP-ACK packet

**DHCP Snooping Option 82 Introduction**

For details on Option 82, refer to “Option 82 Support on DHCP Relay Agent” on page 634.

**Padding content and frame format of Option 82**

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for Switch 5500 Family (enabled with DHCP snooping) are padded as follows:

- sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client’s request.
- sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client’s request.

By default, when Switch 5500 Family serve as DHCP snooping devices, Option 82 adopts the extended format. Refer to Figure 185 and Figure 186 for the extended format of the sub-options (with the default padding contents). That is, the circuit ID or remote ID sub-option defines the type and length of a circuit ID or remote ID.

The remote ID type field and circuit ID type field are determined by the option storage format. They are both set to 0 in the case of HEX format and to 1 in the case of ASCII format.

**Figure 185** Extended format of the circuit ID sub-option

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Length</th>
<th>Circuit ID type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td></td>
<td>Port Index</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 186** Extended format of the remote ID sub-option

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Length</th>
<th>Remote ID type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge MAC Address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In practice, some network devices do not support the type and length identifiers of the Circuit ID and Remote ID sub-options. To interwork with these devices, Switch 5500 Family support Option 82 in the standard format. Refer to Figure 187 and Figure 188 for the standard format of the sub-options (with the default padding contents).
padding contents). In the standard format, the Circuit ID or Remote ID sub-option does not contain the two-byte type and length fields of the circuit ID or remote ID.

**Figure 187** Standard format of the circuit ID sub-option

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Length</th>
<th>VLAN ID</th>
<th>Port Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>15</td>
<td>23</td>
</tr>
</tbody>
</table>

**Figure 188** Standard format of the remote ID sub-option

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Length</th>
<th>Bridge MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

### Mechanism of DHCP-snooping Option 82

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client’s request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see Table 476.

**Table 476** Handling a DHCP packet with Option 82

<table>
<thead>
<tr>
<th>Handling policy</th>
<th>Sub-option configuration</th>
<th>The DHCP Snooping device will...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop</td>
<td>-</td>
<td>Drop the packet.</td>
</tr>
<tr>
<td>Keep</td>
<td>-</td>
<td>Forward the packet without changing Option 82.</td>
</tr>
<tr>
<td>Replace Replace</td>
<td>Neither of the two sub-options is configured</td>
<td>Forward the packet after replacing the original Option 82 with the default content.</td>
</tr>
<tr>
<td></td>
<td>Replace Replace</td>
<td>The storage format of Option 82 content is the one specified with the dhcp-snooping information format command or the default HEX format if this command is not executed.</td>
</tr>
<tr>
<td>Replace Replace</td>
<td>Circuit ID sub-option is configured</td>
<td>Forward the packet after replacing the circuit ID sub-option of the original Option 82 with the configured circuit ID sub-option in ASCII format.</td>
</tr>
<tr>
<td>Replace Replace</td>
<td>Remote ID sub-option is configured</td>
<td>Forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.</td>
</tr>
</tbody>
</table>

When receiving a DHCP client’s request without Option 82, the DHCP snooping device will add the option field with the configured sub-option and then forward the packet. For details, see Table 481.

**Table 477** Handling a DHCP packet without Option 82

<table>
<thead>
<tr>
<th>Sub-option configuration</th>
<th>The DHCP Snooping device will ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neither of the two sub-options is configured</td>
<td>Forward the packet after adding Option 82 with the default contents.</td>
</tr>
<tr>
<td></td>
<td>The format of Option 82 is the one specified with the dhcp-snooping information format command or the default HEX format if this command is not executed.</td>
</tr>
</tbody>
</table>
CHAPTER 55: DHCP SNOOPING CONFIGURATION

The circuit ID and remote ID sub-options in Option 82, which can be configured simultaneously or separately, are independent of each other in terms of configuration sequence.

When the DHCP snooping device receives a DHCP response packet from the DHCP server, the DHCP snooping device will delete the Option 82 field, if contained, before forwarding the packet, or will directly forward the packet if the packet does not contain the Option 82 field.

### Table 477 Handling a DHCP packet without Option 82

<table>
<thead>
<tr>
<th>Sub-option configuration</th>
<th>The DHCP Snooping device will ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit ID sub-option is configured.</td>
<td>Forward the packet after adding Option 82 with the configured circuit ID sub-option in ASCII format.</td>
</tr>
<tr>
<td>Remote ID sub-option is configured.</td>
<td>Forward the packet after adding Option 82 with the configured remote ID sub-option in ASCII format.</td>
</tr>
</tbody>
</table>

A denial-of-service (DoS) attack means an attempt of an attacker sending a large number of forged address requests with different source IP addresses to the server so that the network cannot work normally. The specific effects are as follows:

- The resources on the server are exhausted, so the server does not respond to other requests.
- After receiving such type of packets, a switch needs to send them to the CPU for processing. Too many request packets cause high CPU usage rate. As a result, the CPU cannot work normally.
- The switch can filter invalid IP packets through the DHCP-snooping table and IP static binding table.

### DHCP-snooping table

After DHCP snooping is enabled on a switch, a DHCP-snooping table is generated. It is used to record IP addresses obtained from the DHCP server, MAC addresses, the number of the port through which a client is connected to the DHCP-snooping-enabled device, and the number of the VLAN to which the port belongs to. These records are saved as entries in the DHCP-snooping table.

### IP static binding table

The DHCP-snooping table only records information about clients that obtains IP address dynamically through DHCP. If a fixed IP address is configured for a client, the IP address and MAC address of the client cannot be recorded in the DHCP-snooping table. Consequently, this client cannot pass the IP filtering of the DHCP-snooping table, thus it cannot access external networks.

To solve this problem, the switch supports the configuration of static binding table entries, that is, the binding relationship between IP address, MAC address, and the port connecting to the client, so that packets of the client can be correctly forwarded.

### IP filtering

The switch can filter IP packets in the following two modes:
Filtering the source IP address in a packet. If the source IP address and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.

Filtering the source IP address and the source MAC address in a packet. If the source IP address and source MAC address in the packet, and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.

If a Switch 5500 is enabled with DHCP snooping, the clients connected to it cannot dynamically obtain IP addresses through BOOTP.

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.

To enable DHCP snooping on a Switch 5500 that belongs to an IRF fabric, set the fabric ports on all devices in the fabric to DHCP snooping trusted ports to ensure that the clients connected to each device can obtain IP addresses. In this case, do not configure the ports connecting to the DHCP clients and DHCP server to belong to different units of the fabric; otherwise, the switch cannot record DHCP snooping entries although the clients can obtain IP addresses.

You are not recommended to configure both the DHCP snooping and selective Q-in-Q function on the switch, which may result in the DHCP snooping to function abnormally.

Enable DHCP snooping and specify trusted ports on the switch before configuring DHCP snooping to support Option 82.
Enabling DHCP-snooping Option 82 support

Table 479  DHCP-snooping Option 82 support configuration task list

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling DHCP-snooping Option 82 support” on page 648</td>
<td>Required</td>
</tr>
<tr>
<td>“Configure a handling policy for DHCP packets with Option 82” on page 648</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the storage format of Option 82” on page 648</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configure the circuit ID sub-option” on page 649</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configure the remote ID sub-option” on page 649</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configure the padding format for Option 82” on page 650</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Table 480  Enable DHCP-snooping Option 82 support

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable DHCP-snooping Option 82 support</td>
<td>dhcp-snooping information enable</td>
<td>Required By default, DHCP snooping Option 82 support is disabled.</td>
</tr>
</tbody>
</table>

Configuring a handling policy for DHCP packets with Option 82

Table 481  Configure a handling policy for DHCP packets with Option 82

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure a global handling policy for requests that contain Option 82</td>
<td>dhcp-snooping information strategy (drop</td>
<td>keep</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure a handling policy for requests that contain Option 82 received on the specified interface</td>
<td>dhcp-snooping information strategy (drop</td>
<td>keep</td>
</tr>
</tbody>
</table>

If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Configuring the storage format of Option 82

Switch 5500 Family support the HEX or ASCII format for the Option 82 field.

Table 482  Configure a storage format for the Option 82 field

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>dhcp-snooping information format (hex</td>
<td>ascii)</td>
</tr>
</tbody>
</table>
The dhcp-snooping information format command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the format of the sub-option is ASCII, instead of the one specified with the dhcp-snooping information format command.

### Configure the circuit ID sub-option

Table 483  Configure the circuit ID sub-option

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the circuit ID sub-option in Option 82</td>
<td>dhcp-snooping information [ vlan vlan-id ] circuit-id string string</td>
<td>Optional By default, the circuit ID sub-option contains the VLAN ID and port index related to the port that receives DHCP request packets from DHCP clients</td>
</tr>
</tbody>
</table>

- If you have configured a circuit ID with the vlan vlan-id argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN; while the latter one applies to DHCP messages from other VLANs.

- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the circuit ID sub-option is subject to the one configured on the primary port.

- The circuit ID sub-option configured on a port will not be synchronized or stacked in the case of port aggregation.

### Configuring the remote ID sub-option

You can configure the remote ID sub-option in system view or Ethernet port view:

- In system view, the remote ID takes effect on all interfaces. You can configure Option 82 as the system name (sysname) of the device or any customized character string in the ASCII format.

- In Ethernet port view, the remote ID takes effect only on the current interface. You can configure Option 82 as any customized character string in the ASCII format for different VLANs. That is to say, you can add different configuration rules for packets from different VLANs.

Table 484  Configure the remote ID sub-option in Option 82

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the remote ID sub-option in system view</td>
<td>dhcp-snooping information remote-id { sysname</td>
<td>string string }</td>
</tr>
</tbody>
</table>
CHAPTER 55: DHCP SNOOPING CONFIGURATION

Table 484 Configure the remote ID sub-option in Option 82

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the remote ID sub-option in Ethernet port view</td>
<td>dhcp-snooping information [ vlan vlan-id ] remote-id string</td>
<td>Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the client’s request.</td>
</tr>
</tbody>
</table>

- If you configure a remote ID sub-option in both system view and on a port, the remote ID sub-option configured on the port applies when the port receives a packet, and the global remote ID applies to other interfaces that have no remote ID sub-option configured.

- If you have configured a remote ID with the vlan vlan-id argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.

- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the remote ID is subject to the one configured on the primary port.

- The remote ID configured on a port will neither be synchronized in the case of port aggregation nor support IRF.

Configure the padding format for Option 82

Table 485 Configure the padding format for Option 82

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the padding format</td>
<td>dhcp-snooping information packet-format { extended</td>
<td>Optional By default, the padding format is in extended format.</td>
</tr>
<tr>
<td></td>
<td>standard }</td>
<td></td>
</tr>
</tbody>
</table>

Configuring IP Filtering

Table 486 Configure IP filtering

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable IP filtering</td>
<td>ip check source ip-address [ mac-address ]</td>
<td>Required By default, this function is disabled.</td>
</tr>
<tr>
<td>Create an IP static binding entry</td>
<td>ip source static binding ip-address ip-address [ mac-address mac-address ]</td>
<td>Optional By default, no static binding entry is created.</td>
</tr>
</tbody>
</table>
- Enable DHCP snooping and specify trusted ports on the switch before configuring IP filtering.
- Do not configure IP filtering on the ports of an aggregation group.
- To create a static binding after IP filtering is enabled with the mac-address keyword specified on a port, the mac-address argument must be specified; otherwise, the packets sent from this IP address cannot pass the IP filtering.
- A static entry has a higher priority than the dynamic DHCP snooping entry that has the same IP address as the static one. That is, if the static entry is configured after the dynamic entry is recorded, the static entry overwrites the dynamic entry; if the static entry is configured before DHCP snooping is enabled, no DHCP client can obtain the IP address of the static entry, that is, the dynamic DHCP snooping entry cannot be generated.
- The VLAN ID of the IP static binding configured on a port is the default VLAN ID of the port.

DHCP Snooping Configuration Example

DHCP Snooping Option 82 Support Configuration Example

Network requirements

As shown in Figure 189, Ethernet 1/0/5 of the switch is connected to the DHCP server, and Ethernet 1/0/1, Ethernet 1/0/2, and Ethernet 1/0/3 are respectively connected to Client A, Client B, and Client C.

- Enable DHCP snooping on the switch.
- Specify Ethernet 1/0/5 on the switch as a trusted port for DHCP snooping.
- Enable DHCP-snooping Option 82 support on the switch and set the remote ID field in Option 82 to the system name of the switch. Set the circuit ID sub-option to abcd in DHCP packets from VLAN 1 on Ethernet 1/0/3.

Network diagram

Figure 189  Network diagram for DHCP-snooping Option 82 support configuration
### Configuration procedure

- # Enable DHCP snooping on the switch.
  
  `<Switch> system-view
  [Switch] dhcp-snooping

- # Specify Ethernet 1/0/5 as the trusted port.
  
  `[Switch] interface Ethernet 1/0/5
  [Switch-Ethernet1/0/5] dhcp-snooping trust
  [Switch-Ethernet1/0/5] quit

- # Enable DHCP-snooping Option 82 support.
  
  `[Switch] dhcp-snooping information enable

- # Set the remote ID sub-option in Option 82 to the system name (sysname) of the DHCP snooping device.
  
  `[Switch] dhcp-snooping information remote-id sysname

- # Set the circuit ID sub-option in DHCP packets from VLAN 1 to `abcd` on Ethernet 1/0/3.
  
  `[Switch] interface Ethernet 1/0/3
  [Switch-Ethernet1/0/3] dhcp-snooping information vlan 1 circuit-id string abcd

### IP Filtering

#### Configuration Example

### Network requirements

As shown in Figure 190, Ethernet 1/0/1 of the Switch 5500 is connected to the DHCP server and Ethernet 1/0/2 is connected to Host A. The IP address and MAC address of Host A are 1.1.1.1 and 0001-0001-0001 respectively. Ethernet 1/0/3 and Ethernet 1/0/4 are connected to DHCP Client B and Client C.

- Enable DHCP snooping on the switch, and specify Ethernet 1/0/1 as the DHCP snooping trusted port to prevent attacks from unauthorized DHCP servers.
- Enable IP filtering on Ethernet 1/0/2, Ethernet 1/0/3, and Ethernet 1/0/4 to prevent attacks to the server from clients using fake source IP addresses.
- Create static binding entries on the switch, so that Host A using a fixed IP address can access external networks.
Network diagram

Figure 190  Network diagram for IP filtering configuration

Configuration procedure

# Enable DHCP snooping on the switch.

<Switch> system-view
[Switch] dhcp-snooping

# Specify Ethernet 1/0/1 as the trusted port.

[Switch] interface Ethernet1/0/1
[Switch-Ethernet1/0/1] dhcp-snooping trust
[Switch-Ethernet1/0/1] quit

# Enable IP filtering on Ethernet 1/0/2, Ethernet 1/0/3, and Ethernet 1/0/4 to filter packets based on the source IP addresses/MAC addresses.

[Switch] interface Ethernet 1/0/2
[Switch-Ethernet1/0/2] ip check source ip-address mac-address
[Switch-Ethernet1/0/2] quit
[Switch] interface Ethernet1/0/3
[Switch-Ethernet1/0/3] ip check source ip-address mac-address
[Switch-Ethernet1/0/3] quit
[Switch] interface Ethernet 1/0/4
[Switch-Ethernet1/0/4] ip check source ip-address mac-address
[Switch-Ethernet1/0/4] quit

# Create static binding entries on Ethernet 1/0/2 of the switch.

[Switch] interface Ethernet 1/0/2
[Switch-Ethernet1/0/2] ip source static binding ip-address 1.1.1.1 mac-address 0001-0001-0001

After completing the above configuration, you can verify the configurations by executing the display command in any view.
Table 487  Display DHCP snooping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the user IP-MAC address mapping entries recorded by the DHCP snooping function</td>
<td><code>display dhcp-snooping</code></td>
<td>You can execute the <code>display</code> command in any view</td>
</tr>
<tr>
<td>Display the (enabled/disabled) state of the DHCP snooping function and the trusted ports</td>
<td><code>display dhcp-snooping trust</code></td>
<td></td>
</tr>
<tr>
<td>Display the IP static binding table</td>
<td>`display ip source static binding</td>
<td>vlan vlan-id</td>
</tr>
</tbody>
</table>
Introduction to DHCP Packet Rate Limit

To prevent ARP attacks and attacks from unauthorized DHCP servers, ARP packets and DHCP packets will be processed by the switch CPU for validity checking. But, if attackers generate a large number of ARP packets or DHCP packets, the switch CPU will be under extremely heavy load. As a result, the switch cannot work normally and even goes down.

The Switch 5500 supports ARP and DHCP packet rate limit on a port and shut down the port under attack to prevent hazardous impact on the device CPU. For details about ARP packet rate limit, refer to “ARP Configuration” on page 579. The following describes only the DHCP packet rate limit function.

After DHCP packet rate limit is enabled on an Ethernet port, the switch counts the number of DHCP packets received on this port per second. If the number of DHCP packets received per second exceeds the specified value, packets are passing the port at an over-high rate, which implies an attack to the port. In this case, the switch shuts down this port so that it cannot receive any packet, thus protect the switch from attacks.

In addition, the switch supports port state auto-recovery. After a port is shut down due to over-high packet rate, it resumes automatically after a configurable period of time.

When both port state auto-recovery interval for over-high ARP packet rate and port state auto-recovery interval for over-high DHCP packet rate are configured on a port, the shorter one will be the auto-recovery time.

Configuring DHCP Packet Rate Limit

Table 488  Configure rate limit of DHCP packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter port view</td>
<td>interface interface-type</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Enable the DHCP packet rate</td>
<td>dhcp rate-limit enable</td>
<td>Required</td>
</tr>
<tr>
<td>limit function</td>
<td></td>
<td>By default, DHCP packet rate limit is disabled.</td>
</tr>
<tr>
<td>Configure the maximum DHCP</td>
<td>dhcp rate-limit</td>
<td>Optional</td>
</tr>
<tr>
<td>packet rate allowed on the port</td>
<td></td>
<td>By default, the maximum rate is 15 pps.</td>
</tr>
</tbody>
</table>
CHAPTER 56: DHCP PACKET RATE LIMIT CONFIGURATION

Enable the port state auto-recovery function before setting the auto-recovery interval.

You are not recommended to configure DHCP packet rate limit on the ports of an aggregation group.

### Configuring Port State Auto Recovery

<table>
<thead>
<tr>
<th>Table 488 Configure rate limit of DHCP packets</th>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the port state auto-recovery function</td>
<td>dhcp protective-down recover enable</td>
<td>Optional</td>
<td>By default, the port state auto-recovery function is disabled.</td>
</tr>
<tr>
<td>Set the port state auto-recovery interval</td>
<td>dhcp protective-down recover interval interval</td>
<td>Optional</td>
<td>The port state auto-recovery interval is 300 seconds.</td>
</tr>
</tbody>
</table>

#### Example

**Network requirements**

As shown in Figure 191, Ethernet 1/0/1 of the Switch 5500 is connected to the DHCP server. Ethernet 1/0/2 is connected to client B and Ethernet 1/0/11 is connected to client A.

- Enable DHCP snooping on the switch, and specify Ethernet 1/0/1 as the DHCP snooping trusted port to prevent attacks from unauthorized DHCP servers.
- Configure DHCP packet rate limit on Ethernet 1/0/11 and set the maximum DHCP packet rate allowed on the port to 100 pps.
- Set the port state auto-recovery interval to 30 seconds on the switch.

#### Table 489 Configure port state auto recovery

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable port state auto-recovery</td>
<td>dhcp protective-down recover enable</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the port state auto-recovery interval</td>
<td>dhcp protective-down recover interval interval</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Networking diagram

Figure 191  Network diagram for DHCP packet rate limit configuration

Configuration procedure

# Enable DHCP snooping on the switch.
<Switch> system-view
[Switch] dhcp-snooping

# Specify Ethernet 1/0/1 as the trusted port.
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] dhcp-snooping trust
[Switch-Ethernet1/0/1] quit

# Enable auto recovery.
[5500] dhcp protective-down recover enable

# Set the port state auto-recovery interval to 30 seconds.
[5500] dhcp protective-down recover interval 30

# Enter port view.
[5500] interface Ethernet 1/0/11

# Enable DHCP packet rate limit on Ethernet 1/0/11.
[5500-Ethernet1/0/11] dhcp rate-limit enable

# Set the maximum DHCP packet rate allowed on Ethernet 1/0/11 to 100 pps.
[5500-Ethernet1/0/11] dhcp rate-limit 100
DHCP/BOOTP CLIENT CONFIGURATION

Introduction to the DHCP Client
After you specify a VLAN interface as a DHCP client, the device can use DHCP to obtain parameters such as IP address dynamically from the DHCP server, which facilitates user configuration and management.

Refer to “Obtaining IP Addresses Dynamically” on page 598 for the process of how a DHCP client dynamically obtains an IP address through DHCP.

Introduction to BOOTP Client
After you specify an interface as a Bootstrap Protocol (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 sends a request to the BOOTP server, the BOOTP server will search for the BOOTP parameter file and return it to the client.

A BOOTP client dynamically obtains an IP address from a BOOTP server in the following way:

1. The BOOTP client broadcasts a BOOTP request, which contains its own MAC address.
2. The BOOTP server receives the request and searches for the corresponding IP address according to the MAC address of the BOOTP client and sends the information in a BOOTP response to the BOOTP client.
3. The BOOTP client obtains the IP address from the received response.

Because a DHCP server can interact with a BOOTP client, you can use the DHCP server to assign an IP address to the BOOTP client, without needing to configure any BOOTP server.

Configuring a DHCP/BOOTP Client

<table>
<thead>
<tr>
<th>Table 490</th>
<th>Configure a DHCP/BOOTP client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
</tr>
</tbody>
</table>
Currently, a Switch 5500 functioning as the DHCP client can use an IP address for 24 days at most. That is, the DHCP client can obtain an address lease for no more than 24 days even though the DHCP server offers a longer lease period.

If a switch belongs to an IRF fabric, you need to enable the UDP-helper function on the switch before configuring its VLAN interfaces to obtain IP addresses through DHCP.

To improve security and avoid malicious attack to the unused SOCKETs, Switch 5500s provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The specific implementation is:

- Using the `ip address dhcp-alloc` command enables the DHCP client, and UDP port 68.
- Using the `undo ip address dhcp-alloc` command disables the DHCP client, and UDP port 68.

### DHCP Client Configuration Example

**Network requirements**

Using DHCP, VLAN-interface 1 of Switch B is connected to the LAN to obtain an IP address from the DHCP server.

**Network diagram**

See Figure 177.

**Configuration procedure**

The following describes only the configuration on Switch B serving as a DHCP client.

```
# Configure VLAN-interface 1 to dynamically obtain an IP address by using DHCP.
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address dhcp-alloc
```

### BOOTP Client Configuration Example

**Network requirement**

Switch B’s port belonging to VLAN1 is connected to the LAN. VLAN interface 1 obtains an IP address from the DHCP server by using BOOTP.

**Network diagram**

See Figure 177.
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>
<thead>
<tr>
<th>Displaying DHCP/BOOTP Client Configuration</th>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Display related information on a DHCP client</td>
<td>display dhcp client [ verbose ]</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Display related information on a BOOTP client</td>
<td>display bootp client [ interface Vlan-interface vlan-id ]</td>
<td>Available in any view</td>
</tr>
</tbody>
</table>
ACL Overview

As the network scale and network traffic are increasingly growing, security control and bandwidth assignment play a more and more important role in network management. Filtering data packets can prevent a network from being accessed by unauthorized users efficiently while controlling network traffic and saving network resources. Access Control Lists (ACL) are often used to filter packets with configured matching rules.

Upon receiving a packet, the switch compares the packet with the rules of the ACL applied on the current port to permit or discard the packet.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

ACLs classify packets using a series of conditions known as rules. The conditions can be based on source addresses, destination addresses and port numbers carried in the packets.

According to their application purposes, ACLs fall into the following four types.

- Basic ACL. Rules are created based on source IP addresses only.
- Advanced ACL. Rules are created based on the Layer 3 and Layer 4 information such as the source and destination IP addresses, type of the protocols carried by IP, protocol-specific features, and so on.
- Layer 2 ACL. Rules are created based on the Layer 2 information such as source and destination MAC addresses, VLAN priorities, type of Layer 2 protocol, and so on.
- User-defined ACL. An ACL of this type matches packets by comparing the strings retrieved from the packets with specified strings. It defines the byte it begins to perform and operation with the mask on the basis of packet headers.

ACL Matching Order

An ACL can contain multiple rules, each of which matches specific type of packets. So the order in which the rules of an ACL are matched needs to be determined.

The rules in an ACL can be matched in one of the following two ways:

- **config**: where rules in an ACL are matched in the order defined by the user.
- **auto**: where rules in an ACL are matched in the order determined by the system, namely the depth-first rule (Layer 2 ACLs and user-defined ACLs do not support this feature).
For depth-first rule, there are two cases:

**Depth-first match order for rules of a basic ACL**

1. Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
2. Fragment keyword: A rule with the fragment keyword is prior to others.
3. If the above two conditions are identical, the earlier configured rule applies.

**Depth-first match order for rules of an advanced ACL**

1. Protocol range: A rule which has specified the types of the protocols carried by IP is prior to others.
2. Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
3. Range of destination IP address. The smaller the destination IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
4. Range of Layer 4 port number, that is, TCP/UDP port number. The smaller the range, the higher the match priority.
5. Number of parameters: the more the parameters, the higher the match priority.

If rule A and rule B are still the same after comparison in the above order, the weighting principles will be used in deciding their priority order. Each parameter is given a fixed weighting value. This weighting value and the value of the parameter itself will jointly decide the final matching order. Involved parameters with weighting values from high to low are `icmp-type`, `established`, `dscp`, `tos`, `precedence`, `fragment`. Comparison rules are listed below.

- The smaller the weighting value left, which is a fixed weighting value minus the weighting value of every parameter of the rule, the higher the match priority.
- If the types of parameter are the same for multiple rules, then the sum of parameters’ weighting values of a rule determines its priority. The smaller the sum, the higher the match priority.

---

**Ways to Apply an ACL on a Switch**

**Being applied to the hardware directly**

In the switch, an ACL can be directly applied to hardware for packet filtering and traffic classification. In this case, the rules in an ACL are matched in the order determined by the hardware instead of that defined in the ACL. For the Switch 5500, the later the rule applies, the higher the match priority.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

**Being referenced by upper-level software**

ACLs can also be used to filter and classify the packets to be processed by software. In this case, the rules in an ACL can be matched in one of the following two ways:
ACL Configuration

- `config`, where rules in an ACL are matched in the order defined by the user.
- `auto`, where the rules in an ACL are matched in the order determined by the system, namely the **depth-first** order (Layer 2 ACLs and user-defined ACLs do not support this feature).

When applying an ACL in this way, you can specify the order in which the rules in the ACL are matched. The match order cannot be modified once it is determined, unless you delete all the rules in the ACL and define the match order.

An ACL can be referenced by upper-layer software:

- Referenced by routing policies
- Used to control Telnet, SNMP and Web login users

When an ACL is directly applied to hardware for packet filtering, the switch will permit packets if the packets do not match the ACL.

When an ACL is referenced by upper-layer software to control Telnet, SNMP and Web login users, the switch will deny packets if the packets do not match the ACL.

**Types of ACLs Supported by Switch 5500 Family**

The following types of ACLs are supported by the Switch 5500:

- Basic ACL
- Advanced ACL
- Layer 2 ACL
- User-defined ACL

In addition, ACLs defined on the Switch 5500 can be applied to hardware directly or referenced by upper-layer software for packet filtering.

**ACL Configuration**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Time Range</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring Basic ACL</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring Advanced ACL</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring Layer 2 ACL</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring User-defined ACL</td>
<td>Required</td>
</tr>
<tr>
<td>Applying ACLs on Ports</td>
<td>Required</td>
</tr>
<tr>
<td>Applying ACLs to a VLAN</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring Time Range**

Time ranges can be used to filter packets. You can specify a time range for each rule in an ACL. A time range-based ACL takes effect only in specified time ranges. Only after a time range is configured and the system time is within the time range, can an ACL rule take effect.

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.

An absolute time range on the Switch 5500 Family can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

Configuration Procedure

Table 492 Configure a time range

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a time range</td>
<td>time-range time-name { start-time to end-time days-of-the-week [ from start-time start-date ] [ to end-time end-date ]</td>
<td>Required</td>
</tr>
</tbody>
</table>

Note that:

- If only a periodic time section is defined in a time range, the time range is active only when the system time is within the defined periodic time section. If multiple periodic time sections are defined in a time range, the time range is active only when the system time is within one of the periodic time sections.

- If only an absolute time section is defined in a time range, the time range is active only when the system time is within the defined absolute time section. If multiple absolute time sections are defined in a time range, the time range is active only when the system time is within one of the absolute time sections.

- If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range contains an absolute time section ranging from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section ranging from 12:00 to 14:00 on every Wednesday. This time range is active only when the system time is within the range from 12:00 to 14:00 on every Wednesday in 2004.

- If the start time is not specified, the time section starts from 1970/1/1 00:00 and ends on the specified end date. If the end date is not specified, the time section starts from the specified start date to 2100/12/31 23:59.

Configuration Example

# Define a periodic time range that spans from 8:00 to 18:00 on Monday through Friday.

<5500> system-view
[5500] time-range test 8:00 to 18:00 working-day
[5500] display time-range test
Current time is 13:27:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
08:00 to 18:00 working-day

# Define an absolute time range spans from 15:00 1/28/2006 to 15:00 1/28/2008.
ACL Configuration

System View

system-view

time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
display time-range test

Current time is 13:30:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
    From 15:00 Jan/28/2000 to 15:00 Jan/28/2004

Configuring Basic ACL

A basic ACL filters packets based on their source IP addresses.

A basic ACL can be numbered from 2000 to 2999.

Configuration Prerequisites

- To configure a time range-based basic ACL rule, you need to create the corresponding time range first. For information about configuring the time, refer to "Configuring Time Range" on page 665.
- The source IP addresses based on which the ACL filters packets are determined.

Configuration Procedure

Table 493 Define a basic ACL rule

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create an ACL and enter basic</td>
<td>acl number acl-number [ match-order { auto</td>
<td>Required config by default</td>
</tr>
<tr>
<td>ACL view</td>
<td>config }]</td>
<td></td>
</tr>
<tr>
<td>Define an ACL rule</td>
<td>rule [ rule-id ] { deny</td>
<td>permit } [ rule-string ]</td>
</tr>
<tr>
<td>Configure a description string</td>
<td>description text</td>
<td>Optional Not configured by default</td>
</tr>
<tr>
<td>to the ACL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that:

- With the config match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the auto match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the rule-id argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- With the auto match order specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.
Configuration Example

# Configure ACL 2000 to deny packets whose source IP addresses are 192.168.0.1.

```plaintext
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule deny source 192.168.0.1 0
```

# Display the configuration information of ACL 2000.

```plaintext
[5500-acl-basic-2000] display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 1
  rule 0 deny source 192.168.0.1 0
```

Configuring Advanced ACL

An advanced ACL can filter packets by their source and destination IP addresses, the protocols carried by IP, and protocol-specific features such as TCP/UDP source and destination ports, ICMP message type and message code.

An advanced ACL can be numbered from 3000 to 3999. Note that ACL 3998 and ACL 3999 cannot be configured because they are reserved for cluster management.

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint (DSCP).

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined for basic ACLs.

Configuration Prerequisites

- To configure a time range-based advanced ACL rule, create the corresponding time ranges first, as described in the section entitled “Configuring Time Range” on page 665.
- Determine the settings to be specified in the rule, such as source and destination IP addresses, the protocols carried by IP, and protocol-specific features.

Configuration Procedure

Table 494  Define an advanced ACL rule

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Create an advanced ACL and enter advanced ACL view | acl number acl-number [ match-order ( auto | Required
|                                        | config ) ]                          | config by default               |
| Define an ACL rule                     | rule [ rule-id ] { permit | deny } protocol [ rule-string ] | Required
|                                        |                                     | For information about protocol and rule-string, refer to ACL Commands. |
| Assign a description string to the ACL rule | rule rule-id comment text          | Optional
|                                        |                                     | No description by default       |
ACL Configuration

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the **rule-id** argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- If the ACL is created with the **auto** keyword specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

**Configuration Example**

# Configure ACL 3000 to permit the TCP packets sourced from the network 129.9.0.0/16 and destined for the network 202.38.160.0/24 and with the destination port number being 80.

```plaintext
<5500> system-view
[5500] acl number 3000
[5500-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
```

# Display the configuration information of ACL 3000.

```plaintext
[5500-acl-adv-3000] display acl 3000
Advanced ACL  3000, 1 rule
Acl's step is 1
  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
```

**Configuring Layer 2 ACL**

Layer 2 ACLs filter packets according to their Layer 2 information, such as the source and destination MAC addresses, VLAN priority, and Layer 2 protocol types.

A Layer 2 ACL can be numbered from 4000 to 4999.

**Configuration Prerequisites**

- To configure a time range-based Layer 2 ACL rule, create the corresponding time ranges first, as described in “Configuring Time Range” on page 665.
- Determine the settings to be specified in the rule, such as source and destination MAC addresses, VLAN priorities, and Layer 2 protocol types.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a description string to the ACL</td>
<td><strong>description</strong> text</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No description by default</td>
</tr>
</tbody>
</table>
Configuration Procedure

Table 495 Define a Layer 2 ACL rule

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a Layer 2 ACL and enter layer 2 ACL view</td>
<td>acl number acl-number</td>
<td>Required</td>
</tr>
<tr>
<td>Define an ACL rule</td>
<td>rule [ rule-id ] { permit</td>
<td>deny } rule-string</td>
</tr>
<tr>
<td>Assign a description string to the ACL rule</td>
<td>rule rule-id comment text</td>
<td>Optional</td>
</tr>
<tr>
<td>Assign a description string to the ACL</td>
<td>description text</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Note that:

- You can modify any existent rule of the Layer2 ACL and the unmodified part of the ACL remains.
- If you do not specify the rule-id argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

Configuration Example

# Configure ACL 4000 to deny packets sourced from the MAC address 000d-88f5-97ed, destined for the MAC address 0011-4301-991e, and with their 802.1p priority being 3.

<5500> system-view
[5500] acl number 4000
[5500-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed ffff-ffff-ffff dest 0011-4301-991e ffff-ffff-ffff

# Display the configuration information of ACL 4000.

[5500-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL 4000, 1 rule
Acl’s step is 1
   rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-ffff dest 0011-4301-991e ffff-ffff-ffff

Configuring User-defined ACL

A user-defined ACL filters packets by comparing specific bytes in packet headers with specified string.

A user-defined ACL can be numbered from 5000 to 5999.
Configuration Prerequisites
To configure a time range-based user-defined ACL rule, define the corresponding time ranges first, as described in “Configuring Time Range” on page 665.

Configuration Procedure

Table 496 Define a user-defined ACL rule

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a user-defined ACL</td>
<td>acl number acl-number</td>
<td>Required</td>
</tr>
<tr>
<td>and enter user-defined ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>view</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define an ACL rule</td>
<td>rule [ rule-id ] { permit</td>
<td>deny } [ rule-string rule-mask offset ] &amp;&lt;1-8&gt; [ time-range time-name ]</td>
</tr>
<tr>
<td>Define a comment for the</td>
<td>rule rule-id comment text</td>
<td>Optional</td>
</tr>
<tr>
<td>ACL rule</td>
<td></td>
<td>No description by default</td>
</tr>
<tr>
<td>Define a description for</td>
<td>description text</td>
<td>Optional</td>
</tr>
<tr>
<td>the ACL</td>
<td></td>
<td>No description by default</td>
</tr>
</tbody>
</table>

For the Switch 5500, when configuring a rule that matches specific fields of packets, note that:

- If VLAN-VPN is not enabled, each packet in the switch carries one VLAN tag, which is 4 bytes long.
- If VLAN-VPN is enabled on a port, each packet in the switch carries two VLAN tags, which is 8 bytes long.

For the Switch 5500G, when configuring a rule that matches specific fields of packets, note that each packet in the switch carries two VLAN tags, which is 8 bytes long.

Note that:

- You can modify any existent rule of a user-defined ACL. If you modify only the time range and/or action, the unmodified parts of the rule remain the same. If you modify the rule-string rule-mask offset combinations, however, the new combinations will replace all of the original ones.
- If you do not specify the rule-id argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
CHAPTER 58: ACL CONFIGURATION

Configuration Example

# Configure ACL 5000 to deny all the TCP packets. Where TCP protocol number is 06, mask is ff, and offset is 27 (for the Switch 5500) and 31 (for the Switch 5500G).

```
<5500> system-view
[5500] acl number 5000
[5500-acl-user-5000] rule deny 06 ff 27
```

# Display the configuration information of ACL 5000.

```
[5500-acl-user-5000] display acl 5000
User defined ACL 5000, 1 rule
Acl's step is 1
  rule 0 deny 06 ff 27
```

Applying ACLs on Ports

By applying ACLs on ports, you can filter the packets on the corresponding ports.

Configuration Prerequisites

Define your ACL before applying it to a port as defined in the sections entitled “Configuring Basic ACL” on page 667, “Configuring Advanced ACL” on page 668, “Configuring Layer 2 ACL” on page 669, and “Configuring User-defined ACL” on page 670.

Configuration Procedure

Table 497 Apply an ACL on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
</tbody>
</table>
| Apply an ACL on the port   | Switch 5500: packet-filter { inbound | Required
|                            | outbound } acl-rule                          | For information about acl-rule, refer to the ACL Commands in the Switch 5500 Family Command Reference Guide. |
|                            | Switch 5500G: packet-filter inbound acl-rule |                                                 |

Configuration Example

# Apply ACL 2000 on Ethernet 1/0/1 to filter inbound packets.

```
<5500> system-view
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] packet-filter inbound ip-group 2000
```

Applying ACLs to a VLAN

By applying ACLs to a VLAN, you can filter the packets on all the ports in the VLAN.

Configuration Prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs as defined in the sections entitled “Configuring Basic ACL” on page 667, “Configuring Advanced ACL” on page 668, “Configuring Layer 2 ACL” on page 669, and “Configuring User-defined ACL” on page 670.
Configuration Procedure

Table 498  Apply ACL rules to a VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>_</td>
</tr>
<tr>
<td>Apply ACL rules to a VLAN</td>
<td>Switch 5500:</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td>packet-filter vlan vlan-id {</td>
<td>For information about acl-rule, refer to ACL commands as defined in the</td>
</tr>
<tr>
<td></td>
<td>inbound</td>
<td>outbound } acl-rule</td>
</tr>
<tr>
<td></td>
<td>Switch 5500G:</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td>packet-filter vlan vlan-id</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td>inbound acl-rule</td>
<td>_</td>
</tr>
</tbody>
</table>

Configuration Example

# Apply ACL 2000 in the inbound direction of VLAN 1 to filter packets.

<5500> system-view
[5500] packet-filter vlan 1 inbound ip-group 2000

Displaying and Maintaining the ACL Configuration

After completing the above configuration, you can execute the display commands in any view to view the ACL running information and verify the configuration.

Table 499  Display ACL configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a configured ACL or all</td>
<td>display acl { all</td>
<td>acl-number }</td>
</tr>
<tr>
<td>the ACLs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display a time range or all the</td>
<td>display time-range { all</td>
<td></td>
</tr>
<tr>
<td>time ranges</td>
<td>time-name }</td>
<td></td>
</tr>
<tr>
<td>Display the information about</td>
<td>display packet-filter {</td>
<td></td>
</tr>
<tr>
<td>packet filtering</td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>unitid }</td>
</tr>
<tr>
<td></td>
<td>unit-id }</td>
<td></td>
</tr>
<tr>
<td>Display information about</td>
<td>display drv qacl_resource</td>
<td></td>
</tr>
<tr>
<td>ACL resources</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Examples for Upper-layer Software Referencing ACLs

Example for Controlling Telnet Login Users by Source IP

Network requirements

Apply an ACL to permit users with the source IP address of 10.110.100.52 to telnet to the switch.
Network diagram

**Figure 192** Network diagram for controlling Telnet login users by source IP

![Network diagram for controlling Telnet login users by source IP](image)

**Configuration procedure**

# Define ACL 2000.

```plaintext
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[5500-acl-basic-2000] quit
```

# Reference ACL 2000 on VTY user interface to control Telnet login users.

```plaintext
[5500] user-interface vty 0 4
[5500-ui-vty0-4] acl 2000 inbound
```

**Example for Controlling Web Login Users by Source IP**

**Network requirements**

Apply an ACL to permit Web users with the source IP address of 10.110.100.46 to log in to the switch through HTTP.

**Network diagram**

**Figure 193** Network diagram for controlling Web login users by source IP

![Network diagram for controlling Web login users by source IP](image)

**Configuration procedure**

# Define ACL 2001.

```plaintext
<5500> system-view
[5500] acl number 2001
[5500-acl-basic-2001] rule 1 permit source 10.110.100.46 0
[5500-acl-basic-2001] quit
```
Example for Applying ACLs to Hardware

Basic ACL Configuration Example

Network requirements
PC1 and PC2 connect to the switch through Ethernet 1/0/1. PC1’s IP address is 10.1.1.1. Apply an ACL on Ethernet 1/0/1 to deny packets with the source IP address of 10.1.1.1 from 8:00 to 18:00 everyday.

Network diagram

Figure 194  Network diagram for basic ACL configuration

Configuration procedure
# Define a periodic time range that is active from 8:00 to 18:00 everyday.
<5500> system-view
[5500] time-range test 8:00 to 18:00 daily

# Define ACL 2000 to filter packets with the source IP address of 10.1.1.1.

[5500] acl number 2000
[5500-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[5500-acl-basic-2000] quit

# Apply ACL 2000 on Ethernet 1/0/1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] packet-filter inbound ip-group 2000

Advanced ACL Configuration Example

Network requirements
Different departments of an enterprise are interconnected through a switch. The IP address of the wage query server is 192.168.1.2. The R&D department is connected to Ethernet 1/0/1 of the switch. Apply an ACL to deny requests from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).
Network diagram

Figure 195  Network diagram for advanced ACL configuration

[Diagram showing network connections]

Configuration procedure

# Define a periodic time range that is active from 8:00 to 18:00 everyday.

<5500> system-view
[5500] time-range test 8:00 to 18:00 working-day

# Define ACL 3000 to filter packets destined for wage query server.

[5500] acl number 3000
[5500-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[5500-acl-adv-3000] quit

# Apply ACL 3000 on Ethernet 1/0/1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] packet-filter inbound ip-group 3000

Layer 2 ACL

Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. PC 1’s MAC address is 0011-0011-0011. Apply an ACL to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012 from 8:00 to 18:00 everyday.

Network diagram

Figure 196  Network diagram for Layer 2 ACL

[Diagram showing network connections]
Configuration procedure

# Define a periodic time range that is active from 8:00 to 18:00 everyday.

<5500> system-view
[5500] time-range test 8:00 to 18:00 daily

# Define ACL 4000 to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012.

[5500] acl number 4000
[5500-acl-ethernetframe-4000] quit

# Apply ACL 4000 on Ethernet 1/0/1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] packet-filter inbound link-group 4000

User-defined ACL Configuration Example

Network requirements

As shown in Figure 197, PC 1 and PC 2 are connected to the switch through Ethernet 1/0/1 and Ethernet 1/0/2 respectively. They belong to VLAN 1 and access the Internet through the same gateway, which has an IP address of 192.168.0.1 (the IP address of VLAN-interface 1).

Configure a user-defined ACL to deny all ARP packets from PC 1 that use the gateway IP address as the source address from 8:00 to 18:00 everyday.

Network diagram

Figure 197 Network diagram for user-defined ACL

Configuration procedure for the Switch 5500

# Define a periodic time range that is active from 8:00 to 18:00 everyday.

<5500> system-view
[5500] time-range test 8:00 to 18:00 daily

# Define ACL 5000 to deny any ARP packet whose source IP address is 192.168.0.1 from 8:00 to 18:00 everyday (provided that VLAN-VPN is not enabled on any port). In the ACL rule, 0806 is the ARP protocol number, ffff is the mask of the rule, 16 is the protocol type field offset of the internally processed Ethernet frame, c0a80001 is the hexadecimal form of 192.168.0.1, and 32 is the source IP address field offset of the internally processed ARP packet.
[5500] acl number 5000
[5500-acl-user-5000] rule 1 deny 0806 ffff 16 c0a80001 fffffffff 32
    time-range test

# Apply ACL 5000 on Ethernet 1/0/1.

[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] packet-filter inbound user-group 5000

**Configuration procedure for the Switch 5500G**

# Define a periodic time range that is active from 8:00 to 18:00 everyday.

<5500G> system-view
[5500G] time-range test 8:00 to 18:00 daily

# Define ACL 5000G to deny any ARP packet whose source IP address is 192.168.0.1 from 8:00 to 18:00 everyday. In the ACL rule, 0806 is the ARP protocol number, ffff is the mask of the rule, 20 is the protocol type field offset of the internally processed Ethernet frame, c0a80001 is the hexadecimal form of 192.168.0.1, and 36 is the source IP address field offset of the internally processed ARP packet.

[5500G] acl number 5000
[5500G-acl-user-5000] rule 1 deny 0806 ffff 20 c0a80001 fffffffff 36
    time-range test

# Apply ACL 5000G on GigabitEthernet 1/0/1.

[5500G] interface GigabitEthernet1/0/1
[5500G-GigabitEthernet1/0/1] packet-filter inbound user-group 5000

**Example for Applying an ACL to a VLAN**

**Network requirements**

PC1, PC2, and PC3 belong to VLAN 10 and connect to the switch through Ethernet 1/0/1, Ethernet 1/0/2 and Ethernet 1/0/3 respectively. The IP address of the database server is 192.168.1.2. Apply an ACL to deny packets from PCs in VLAN 10 to the database server from 8:00 to 18:00 in working days.
Network diagram

**Figure 198** Network diagram for applying an ACL to a VLAN

```plaintext
# Define a periodic time range that is active from 8:00 to 18:00 in working days.
<5500> system-view
[5500] time-range test 8:00 to 18:00 working-day

# Define an ACL to deny packets destined for the database server.
[5500] acl number 3000
[5500-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[5500-acl-adv-3000] quit

# Apply ACL 3000 to VLAN 10.
[5500] packet-filter vlan 10 inbound ip-group 3000
```
### Overview

#### Introduction to QoS

Quality of service (QoS) is a concept generally existing in occasions with service supply and demand. It evaluates the ability to meet the need of the customers in service. Generally, the evaluation is not to grade precisely. Its purpose is to analyze the conditions where the service is the best and the conditions where the service still needs improvement and then to make improvements in the specified aspects.

In an internet, QoS evaluates the ability of the network to deliver packets. The evaluation on QoS can be based on different aspects because the network provides various services. Generally speaking, QoS is the evaluation on the service ability to support the core requirements such as delay, jitter, and packet loss ratio in the packet delivery.

#### Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer, email, and FTP.

#### New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long
delay may cause unexpected results. That is, they need to get serviced in time even if congestion occurs.

Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

**Major Traffic Control Techniques**

Traffic identifying, traffic policing (TP), traffic shaping (TS), congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions.

- **Traffic identifying** identifies specific packets based on certain matching rules. It is a prerequisite for differentiated service.
- **TP** confines traffics to a specific specification. You can configure restriction or punishment measures against the traffics exceeding the specification to protect the benefits of carriers and to prevent network resources from being abused.
- **TS** adjusts the output rate of traffic actively. It can enable the traffics to match the capacity of the downstream network devices, so as to prevent packets from being dropped and network congestion.
- **Congestion management** handles resource competition during network congestion. Generally, it adds packets to queues first, and then forwards the packets by using a scheduling algorithm.
- **Congestion avoidance** monitors the use of network resources and drops packets actively when congestion reaches certain degree. It relieves network load by adjusting traffics.

Traffic identifying is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. TP, TS, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

**QoS Supported By Switch 5500 Family**

**Traffic Identifying**

Traffic here refers to service traffic; that is, all the packets passing the switch.

Traffic identifying means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.

In traffic identifying, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic identifying policies to identify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Normally, traffic identifying is done by checking the information carried in packet header. Packet payload is rarely adopted for traffic identifying. The identifying rule is unlimited in range. It can be a quintuplet...
consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

**Precedence**

**IP precedence, ToS precedence, and DSCP precedence**

**Figure 199** DS field and ToS byte

The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service code point (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

**Table 500** Description of IP Precedence

<table>
<thead>
<tr>
<th>IP Precedence (decimal)</th>
<th>IP Precedence (binary)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>Routine</td>
</tr>
<tr>
<td>1</td>
<td>001</td>
<td>priority</td>
</tr>
<tr>
<td>2</td>
<td>010</td>
<td>immediate</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>flash</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>flash-override</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>critical</td>
</tr>
<tr>
<td>6</td>
<td>110</td>
<td>internet</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>network</td>
</tr>
</tbody>
</table>

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 501 Description of DSCP precedence values

<table>
<thead>
<tr>
<th>DSCP value (decimal)</th>
<th>DSCP value (binary)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>101110</td>
<td>ef</td>
</tr>
<tr>
<td>10</td>
<td>001010</td>
<td>af11</td>
</tr>
<tr>
<td>12</td>
<td>001100</td>
<td>af12</td>
</tr>
<tr>
<td>14</td>
<td>001110</td>
<td>af13</td>
</tr>
<tr>
<td>18</td>
<td>010010</td>
<td>af21</td>
</tr>
<tr>
<td>20</td>
<td>010100</td>
<td>af22</td>
</tr>
<tr>
<td>22</td>
<td>010110</td>
<td>af23</td>
</tr>
<tr>
<td>26</td>
<td>011010</td>
<td>af31</td>
</tr>
<tr>
<td>28</td>
<td>011100</td>
<td>af32</td>
</tr>
<tr>
<td>30</td>
<td>011110</td>
<td>af33</td>
</tr>
<tr>
<td>34</td>
<td>100010</td>
<td>af41</td>
</tr>
<tr>
<td>36</td>
<td>100100</td>
<td>af42</td>
</tr>
<tr>
<td>38</td>
<td>100110</td>
<td>af43</td>
</tr>
<tr>
<td>8</td>
<td>001000</td>
<td>cs1</td>
</tr>
<tr>
<td>16</td>
<td>010000</td>
<td>cs2</td>
</tr>
<tr>
<td>24</td>
<td>011000</td>
<td>cs3</td>
</tr>
<tr>
<td>32</td>
<td>100000</td>
<td>cs4</td>
</tr>
<tr>
<td>40</td>
<td>101000</td>
<td>cs5</td>
</tr>
<tr>
<td>48</td>
<td>110000</td>
<td>cs6</td>
</tr>
<tr>
<td>56</td>
<td>111000</td>
<td>cs7</td>
</tr>
<tr>
<td>0</td>
<td>000000</td>
<td>be (default)</td>
</tr>
</tbody>
</table>

### 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 200 An Ethernet frame with an 802.1Q tag header

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Source Address</th>
<th>802.1Q header</th>
<th>Length/Type</th>
<th>Data</th>
<th>FCS (CRC-32)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bytes</td>
<td>6 bytes</td>
<td>4 bytes</td>
<td>2 bytes</td>
<td>46~1517 bytes</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>

As shown in the figure above, each host supporting 802.1Q protocol adds a 4-byte 802.1Q tag header after the source address of the former Ethernet frame header when sending packets. The 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag
control information (TCI, two bytes in length). Figure 201 describes the detailed contents of an 802.1Q tag header.

![Figure 201 802.1Q tag headers](image)

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 502 Description of 802.1p priority

<table>
<thead>
<tr>
<th>802.1p priority (decimal)</th>
<th>802.1p priority (binary)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>best-effort</td>
</tr>
<tr>
<td>1</td>
<td>001</td>
<td>background</td>
</tr>
<tr>
<td>2</td>
<td>010</td>
<td>spare</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>excellent-effort</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>controlled-load</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>video</td>
</tr>
<tr>
<td>6</td>
<td>110</td>
<td>voice</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>network-management</td>
</tr>
</tbody>
</table>

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

### Priority Trust Mode

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules. The local precedence is locally significant precedence that the switch assigns to the packet. It corresponds to an output queue. Packets with higher local precedence values take precedence over those with lower precedence values and will be processed preferentially.

When a packet carrying no 802.1q tag reaches a switch, the switch uses the priority of the receiving port as the 802.1p priority of the packet and maps the priority to the corresponding local precedence.

For a packet carrying an 802.1q tag, a switch provides the following two priority trust modes:

- **Trusting packet priority**

  In this mode, the switch searches for the local precedence corresponding to the 802.1p priority of the packet in the 802.1p-to-local precedence mapping table and assign the local precedence to the packet.

- **Trusting port priority**
In this mode, the switch searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table and assign the local precedence to the packet.

Table 503 shows the default 802.1p priority-to-local precedence mapping table.

**Table 503** 802.1p priority-to-local precedence mapping table

<table>
<thead>
<tr>
<th>802.1p priority</th>
<th>Local precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

**Protocol Priority** Protocol packets carry their own priority. You can modify the priority of a protocol packet to implement QoS.

**Priority Marking** The priority marking function is to use ACL rules in traffic identifying and reassign the priority for the packets matching the ACL rules.

**TP** The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, traffic can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

TP (traffic policing) is a kind of traffic control policy used to limit the traffic and the resource occupied by supervising the traffic. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when TP is performed. Normally, token bucket is used for traffic evaluation.

**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 the traffic with the token bucket

When token bucket is used for traffic evaluation, the number of the tokens in the token bucket determines the amount of the packets that can be forwarded. 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.

Parameters concerning token bucket 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.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

**TP**

The typical application of TP is to supervise specific traffic into the network and limit it to 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, TP can choose to drop the packets or to reset the priority of the packets.
TP is widely used in policing the traffic into the network of internet service providers (ISPs). TP can identify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

- **Drop.** Drop the packet whose evaluation result is nonconforming.
- **Modify the DSCP precedence and forward.** Modify the DSCP precedence of the packets whose evaluation result is nonconforming and then forward them.

**Line Rate**

Line Rate (LR) refers to limiting the total rate of inbound or outbound packets on a port. LR can be implemented through token buckets. That is, if you perform LR configuration for a port, the token bucket determines the way to process the packets to be sent by this port or packets reaching the port. Packets can be sent or received if there are enough tokens in the token bucket; otherwise, they will be dropped.

Compared to TP, LR applies to all the packets passing a port. It is a simpler solution if you want to limit the rate of all the packets passing a port.

**Traffic Redirecting**

Traffic redirecting identifies traffic using ACLs and redirects the matched packets to CPU, the specified ports/aggregation group. By traffic redirecting, you can change the way in which a packet is forwarded to achieve specific purposes.

**VLAN Mapping**

VLAN mapping identifies traffics using ACLs and maps the VLAN tags carrier in matched packets to specific VLAN tags. By employing VLAN mapping on a switch connecting user networks to the carrier network, you can map the VLAN tags of specific user network packets to those of specific VLANs in the carrier network, thus meeting the requirements of the carrier network.

**Queue Scheduling**

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.
In the following section, strict priority (SP) queues, weighted fair queue (WFQ), and weighted round robin (WRR) queues are introduced.

1 SP queuing

*Figure 203* 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 WFQ queuing

*WRR Queuing applies to the Switch 5500 only (not the 5500G).*
Before WFQ is introduced, you must understand fair queuing (FQ) first. FQ is designed for the purpose of sharing network resources fairly and optimizing the delays and delay jitters of all the flows. It takes the interests of all parties into account, such as:

- Different queues are scheduled fairly, so the delay of each flow is balanced globally.
- Both short and long packets are scheduled fairly. When there are multiple long packets and short packets to be sent among different queues, the short packets must be scheduled preferentially, so that the delay jitters of packets of each flow is reduced globally.

Compared with FQ, WFQ takes the priority into account when calculating the scheduling sequence of packets. Statistically speaking, WFQ assigns more scheduling chances to high priority packets than those to low priority packets. WFQ can classify the traffic automatically according to the session information of traffic including the protocol types, source and destination TCP or UDP port numbers, source and destination IP addresses, and priority values in the ToS field. WFQ also provide as many queues as possible to accommodate each flow evenly. Thus, the delay of each flow is balanced globally. When the packets dequeue, WFQ assigns the bandwidth to each flow on the egress according to the traffic precedence or DSCP precedence. The lower the traffic precedence is, the less bandwidth the traffic gets. The higher the traffic precedence is, the more bandwidth the traffic gets. Finally, each queue is polled and the corresponding number of packets is taken out to be sent according to the proportion of bandwidth.

You can use the WFQ algorithm to assign bandwidth to the output queues of a port, and then decide which queue a traffic flows into according to the mapping between the COS value of the traffic and the queue, and also decide how much bandwidth is to be assigned to each traffic.
WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are eight output queues on a port. WRR configures a weight value for each queue, which is \(w_7, w_6, w_5, w_4, w_3, w_2, w_1,\) and \(w_0\). The weight value indicates the proportion of obtaining resources. On a 100 M port, configure the weight value of WRR queue-scheduling algorithm to \(5, 5, 3, 3, 1, 1, 1,\) and \(1\) (corresponding to \(w_7, w_6, w_5, w_4, w_3, w_2, w_1,\) and \(w_0\) in order). In this way, the queue with the lowest priority can get 5 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

**Congestion Avoidance**

This section applies to the Switch 5500 only (not the Switch 5500G)

Congestion may cause network resource unavailable and thus need to be prevented. As a type of flow control mechanism, congestion avoidance aims to relieve network load through traffic adjusting. With congestion avoidance configuration performed, packets are dropped in advance when the utilization of certain network resources (such as output queues or buffer created in the memory) reaches certain degree.

**Traditional packet dropping policy**

Tail drop is adopted in traditional packet drop policies. It drops all the newly arrived packets when the current queue length reaches a specific value.

Such a policy will result in global TCP connection synchronization. If a queue drops packets of multiple TCP connections simultaneously, the TCP connections will turn to the state of congestion avoidance and slow startup for the traffics to be regulated. The traffic peak will then occur in a certain future time. Consequently, the network traffic jitters all the time.
**WRED**

You can use weighted random early detection (WRED) to avoid global TCP session synchronization.

In WRED algorithm, an upper limit and a lower limit are set for each queue, and the packets in a queue are processed as follows.

- When the current queue length is smaller than the lower limit, no packet is dropped;
- When the queue length exceeds the upper limit, all the newly received packets are dropped;
- When the queue length is between the lower limit and the upper limit, the newly received packets are dropped at random. The longer the queue, the more likely the newly received packets may be dropped. However, a maximum drop probability exists.

In WRED, random numbers are generated to determine the packets to be dropped. As the dropping policy is determined by IP precedence, packets with lower precedence are more likely to be dropped.

WRED prevents global TCP session synchronization. It enables other TCP sessions to be free of a TCP session slowed down because of its packets being dropped. In this way, TCP sessions can operate in different rates in any case and the link bandwidth can be fully utilized.

**Traffic-based Traffic Accounting**

The function of traffic-based traffic accounting is to use ACL rules in traffic identifying and perform traffic accounting on the packets matching the ACL rules. You can get the statistics of the packets you are interested in through this function.

**Burst**

The Burst function can provide better packet cache function and traffic forwarding performance. It is suitable for networks where

- Large amount of broadcast/multicast packets and large burst traffic exist.
- Packets of high-rate links are forwarded to low-rate links or packets of multiple links with the equal rates are forwarded to a single link that is of the same rate as that of the incoming links.

Although the burst function helps reduce the packet loss ratio and improve packet processing capability in the networks mentioned above, it may affect QoS performance. So, use this function with caution.

**Traffic mirroring**

Traffic mirroring identifies traffic using ACLs and duplicates the matched packets to the destination mirroring port or CPU depending on your configuration. For information about port mirroring, refer to “Mirroring Configuration” on page 721.
QoS Configuration

Refer to “Priority Trust Mode” on page 685 for an introduction to priority trust mode.

Configuration prerequisites

- The priority trust mode to be adopted is determined.
- The port where priority trust mode is to be configured is determined.
- The port priority value is determined.

Configuration procedure

Table 504 QoS configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring priority trust mode</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the mapping between 802.1p priority and local precedence</td>
<td>Optional</td>
</tr>
<tr>
<td>Setting the priority of protocol packets</td>
<td>Optional</td>
</tr>
<tr>
<td>Marking packet priority</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring TP</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring LR</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring traffic redirecting</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring VLAN mapping</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring queue scheduling</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring WRED</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring Traffic Accounting</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling the burst function</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring traffic mirroring</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Table 505 Configure to trust port priority

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the port priority</td>
<td>priority priority-level</td>
<td>Optional 0 by default</td>
</tr>
</tbody>
</table>

Table 506 Configure to trust packet priority

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure to trust packet priority</td>
<td>priority trust</td>
<td>Required By default, the switch trusts port priority.</td>
</tr>
</tbody>
</table>
**Configuration example**

- Configure to trust port priority on Ethernet 1/0/1 and set the priority of Ethernet 1/0/1 to 7.

**Configuration procedure:**

```plaintext
<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] priority 7
```

- Configure to trust packet priority on Ethernet 1/0/1.

**Configuration procedure:**

```plaintext
<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] priority trust
```

**Configuring the Mapping between 802.1p Priority and Local Precedence**

By modifying the mapping between 802.1p priority and local precedence, you can modify the mapping between 802.1p priority and the output queues, and thus add packets with different priorities to the corresponding output queues.

**Configuration prerequisites**

The mapping between 802.1p priority and local precedence is determined.

**Configuration procedure**

**Table 507** Configure the mapping between 802.1p priority and local precedence

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the mapping between 802.1p priority and local precedence</td>
<td>qos cos-local-precedence-map</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>cos0-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos1-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos2-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos3-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos4-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos5-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos6-map-local-prec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cos7-map-local-prec</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration example**

- Configure the following mapping between 802.1p priority and local precedence: 0 to 2, 1 to 3, 2 to 4, 3 to 1, 4 to 7, 5 to 0, 6 to 5, and 7 to 6.

- Display the configuration.

**Configuration procedure:**

```plaintext
<5500> system-view
[5500] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[5500] display qos cos-local-precedence-map
cos-local-precedence-map:
cos(802.1p) : 0 1 2 3 4 5 6 7
local precedence(queue) : 2 3 4 1 7 0 5 6
```
### Setting the Priority of Protocol Packets

Refer to “Priority Trust Mode” on page 685 for information about priority of protocol packets.

**Configuration prerequisites**
- The protocol type is determined.
- The priority value is determined.

**Configuration procedure**

#### Table 508  Set the priority for specific protocol packets

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Set the priority for specific protocol packets</td>
<td>`protocol-priority protocol-type protocol-type { ip-precedence</td>
<td>dscp dscp-value }`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can modify the IP precedence or DSCP precedence of the corresponding protocol packets.</td>
</tr>
</tbody>
</table>

On a Switch 5500, you can set the priority for protocol packets of Telnet, OSPF, SNMP, and ICMP.

**Configuration example**
- Set the IP precedence of ICMP packets to 3.
- Display the configuration.

Configuration procedure:

```
<5500> system-view
[5500] protocol-priority protocol-type icmp ip-precedence 3
[5500] display protocol-priority
Protocol: icmp
   IP-Precedence: flash(3)
```

### Marking Packet Priority

Refer to “Priority Trust Mode” on page 685 for information about marking packet priority.

Marking packet priority can be implemented in the following two ways:

- Through TP

When configuring TP, you can define the action of marking the DSCP precedence for packets exceeding the traffic specification. Refer to “Configuring TP” on page 697.

- Through the `traffic-priority` command

You can use the `traffic priority` command to mark the IP precedence, 802.1p priority, DSCP precedence, and local precedence of the packets.

**Configuration prerequisites**

The following items are defined or determined before the configuration:
The ACL rules used for traffic identifying are specified. Refer to “ACL Configuration” on page 663.

The type and value of the precedence to be marked for the packets matching the ACL rules are determined.

The port or VLAN on which the configuration is to be performed is determined.

Configuration procedure

Table 509 Configure priority marking on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Mark the priorities for packets matching specific ACL rules</td>
<td>Switch 5500: traffic-priority { inbound</td>
<td>outbound } acl-rule { ( dscp dscp-value</td>
</tr>
<tr>
<td></td>
<td>Switch 5500G: traffic-priority inbound acl-rule { ( dscp dscp-value</td>
<td>ip-precedence { pre-value</td>
</tr>
</tbody>
</table>

Table 510 Configure priority marking on a VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Mark the priorities for the packets belonging to a VLAN and matching specific ACL rules</td>
<td>Switch 5500: traffic-priority vlan vlan-id { inbound</td>
<td>outbound } acl-rule { ( dscp dscp-value</td>
</tr>
<tr>
<td></td>
<td>Switch 5500G: traffic-priority vlan vlan-id inbound acl-rule { ( dscp dscp-value</td>
<td>ip-precedence { pre-value</td>
</tr>
</tbody>
</table>

Configuration example

- Ethernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.0/24 network segment.
- Mark the DSCP precedence as 56 for the packets from the 10.1.1.0/24 network segment.

1 Method I

<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[5500-acl-basic-2000] quit
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] traffic-priority inbound ip-group 2000 dscp 56

2 Method II

<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[5500-acl-basic-2000] quit
[5500] traffic-priority vlan 2 inbound ip-group 2000 dscp 56

Configuring TP

Refer to “TP” on page 686 for information about TP.

Configuration prerequisites

- The ACL rules used for traffic identifying are defined. Refer to “ACL Configuration” on page 663.
- The rate limit for TP, and the actions for the packets exceeding the rate limit are determined.
- The ports that need this configuration are determined.

Configuration procedure

**Table 511** Configure TP

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure TP</td>
<td>Switch 5500:</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>traffic-limit inbound acl-rule</td>
<td>The target-rate argument is</td>
</tr>
<tr>
<td></td>
<td>[ union-effect ] [ egress-port</td>
<td>committed information rate (CIR),</td>
</tr>
<tr>
<td></td>
<td>interface-type interface-number]</td>
<td>and the burst-bucket-size</td>
</tr>
<tr>
<td></td>
<td>target-rate [ burst-bucket</td>
<td>argument is committed burst</td>
</tr>
<tr>
<td></td>
<td>burst-bucket-size ] [ exceed</td>
<td>size (CBS).</td>
</tr>
<tr>
<td></td>
<td>action ]</td>
<td></td>
</tr>
<tr>
<td>Switch 5500G:</td>
<td>traffic-limit inbound acl-rule</td>
<td>By default, TP is disabled.</td>
</tr>
<tr>
<td></td>
<td>[ union-effect ] target-rate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ burst-bucket burst-bucket-size ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ exceed action ]</td>
<td></td>
</tr>
</tbody>
</table>

The granularity of TP is 64 Kbps. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), it will be rounded off to (N+1)*64.

Configuration example

- Ethernet 1/0/1 of the switch is connected to the 10.1.1.0/24 network segment
- Perform TP on the packets from the 10.1.1.0/24 network segment, setting the rate to 128 kbps
- Mark the DSCP precedence as 56 for the inbound packets exceeding the rate limit.

Configuration procedure:
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[5500-acl-basic-2000] quit
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] traffic-limit inbound ip-group 2000 128 exceed remark-dscp 56

**Configuring LR**

Refer to “Line Rate” on page 688 for information about port rate limiting.

**Configuration prerequisites**

- The port on which LR configuration is to be performed is determined.
- The target rate is determined.
- The target direction of rate limiting (inbound or outbound) is determined (Switch 5500 only, not the Switch 5500G).

**Configuration procedure**

**Table 512 Configuring LR**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure LR</td>
<td>Switch 5500: line-rate { inbound</td>
<td>The target-rate argument is committed information rate (CIR), and the burst-bucket-size argument is committed burst size (CBS).</td>
</tr>
<tr>
<td></td>
<td>outbound } target-rate[ burst-bucket burst-bucket-size ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch 5500G: line-rate outbound target-rate [ burst-bucket burst-bucket-size ]</td>
<td>By default, LR is disabled.</td>
</tr>
</tbody>
</table>

**Configuration example**

- Configure LR for inbound packets on Ethernet 1/0/1.
- The rate limit is 1,024 Kbps

Configuration procedure:

<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] line-rate inbound 1024

**Configuring Traffic Redirecting**

Refer to “Traffic Redirecting” on page 688 for information about traffic redirecting.

**Configuration prerequisites**

- The ACL rules used for traffic identifying are defined. Refer to “ACL Configuration” on page 663 for information about defining ACL rules.
- The traffic redirecting destination is determined.
- The ports that need this configuration are determined.
Packets redirected to the CPU are not forwarded.

If the traffic is redirected to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state. Refer to “Port Basic Configuration” on page 159 for information about Combo ports.

If the traffic is configured to be redirected to an aggregation group, the traffic is redirected to the master port of the aggregation group. Refer to “Link Aggregation Configuration” on page 171 for information about aggregation group.

When the traffic redirecting function is used in conjunction with the selective QinQ function, you can specify the untagged keyword as required (that is, remove the outer VLAN tag of a packet after the packet is redirected to the uplink port) in a tree network with a single uplink port (or an aggregation group). Do not specify the untagged keyword in a ring network or a network with multiple uplink ports. Refer to “VLAN-VPN Configuration” on page 943 for information about selective QinQ.

### Configuration example

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Redirect all the packets from the 10.1.1.0/24 network segment to Ethernet 1/0/7.

Configuration procedure:

```plaintext
<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[5500-acl-basic-2000] quit
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] traffic-redirect inbound ip-group 2000 interface Ethernet1/0/7
```
CHAPTER 59: QoS Configuration

Configuring VLAN Mapping

Refer to “VLAN Mapping” on page 688 for information about VLAN mapping.

Configuration prerequisites

- The ACL rules used for traffic identifying are defined. Refer to “ACL Configuration” on page 663 for information about defining ACL rules.
- The ports on which the configuration is to be performed are determined.

Configuration procedure

Table 514  Configure VLAN mapping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure VLAN mapping</td>
<td>traffic-remark-vlanid inbound acl-rule</td>
<td>By default, VLAN mapping is not configured.</td>
</tr>
<tr>
<td></td>
<td>remark-vlan remark-vlanid</td>
<td></td>
</tr>
</tbody>
</table>

Configuration example

Configure VLAN mapping on Ethernet 1/0/1 to map the VLAN IDs carried in the packets matching ACL 4000 to 1001.

Configuration procedure:

<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] traffic-remark-vlanid inbound link-group 4000 remark-vlan 1001

Configuring Queue Scheduling

Refer to “Queue Scheduling” on page 688 for information about queue scheduling.

Configuration prerequisites

The algorithm for queue scheduling to be used and the related parameters are determined.

Configuration procedure

Table 515  Configure queue scheduling in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure queue scheduling</td>
<td>queue-scheduler</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>strict-priority</td>
<td>By default, the queue scheduling algorithm adopted on all the ports is WRR. The default weights of the eight output queues of a port are 1, 2, 3, 4, 5, 9, 13, and 15 (in the order queue 0 through queue 7).</td>
</tr>
<tr>
<td></td>
<td>wrr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue0-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue1-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue2-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue3-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue4-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue5-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue6-weight</td>
<td></td>
</tr>
<tr>
<td></td>
<td>queue7-weight</td>
<td></td>
</tr>
</tbody>
</table>
A Switch 5500 port supports eight output queues. These queue scheduling algorithms are available: SP, WRR, and WFQ. With WRR (or WFQ) adopted, if you set the weight or the bandwidth of one or multiple queues to 0, the switch adds the queue or queues to the SP group where the SP is adopted. For other queues, WRR (or WFQ) still applies. In this case, both SP and WRR (or WFQ) are adopted. In cases where both SP and WRR (or WFQ) queue scheduling algorithms are adopted, the queues in the SP group take precedence over other queues. For example, if queue 0, queue 1, queue 2, and queue 3 are in the SP group, queue 4, queue 5, queue 6, and queue 7 are scheduled using WRR (or WFQ), the switch will schedule the queues in the SP group preferentially by using the SP algorithm. Then queues outside the SP group are scheduled by using WRR (or WFQ) algorithm only when all the queues in the SP group are empty.

- The queue scheduling algorithm specified by using the queue-scheduler command in system view takes effect on all the ports. The queue scheduling algorithm configured in port view must be the same as that configured in system view. Otherwise, the system prompts configuration errors.

- If the weight (or bandwidth value) specified in system view for a queue of WRR queuing or WFQ queuing cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.

- If the weight (or bandwidth value) specified in system view for a queue of SP-WRR queuing or SP-WFQ queuing in the command cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.

- The display queue-scheduler command cannot display the queue weight (or bandwidth value) specified in Ethernet port view.

### Configuration example

- Adopts WRR for queue scheduling, setting the weights of the output queues to 2, 2, 3, 3, 4, 4, 5, and 5 (in the order queue 0 through queue 7).

- Verify the configuration.
Configuration procedure:

```
<5500> system-view
[5500] queue-scheduler wrr 2 2 3 3 4 4 5 5
[5500] display queue-scheduler
  Queue scheduling mode: weighted round robin
  weight of queue 0: 2
  weight of queue 1: 2
  weight of queue 2: 3
  weight of queue 3: 3
  weight of queue 4: 4
  weight of queue 5: 4
  weight of queue 6: 5
  weight of queue 7: 5
```

### Configuring WRED

Refer to “Congestion Avoidance” on page 691 for information about WRED.

> This command is valid on the Switch 5500 only, no the Switch 5500G.

**Configuration prerequisites**

- The indexes of queues to be dropped at random, the queue length that starts the drop action, and the drop probability are determined.
- The ports that need this configuration are determined.

**Configuration procedure**

**Table 517  Configure WRED**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure WRED</td>
<td>wred queue-index qstart probability</td>
<td>Required By default, WRED is not configured.</td>
</tr>
</tbody>
</table>

**Configuration example**

Configure WRED for queue 2 of Ethernet 1/0/1 to drop the packets in queue 2 randomly when the number of packets in queue 2 exceeds 64, setting the dropping probability being 20%.

Configuration procedure:

```
<5500> system-view
[5500] interface Ethernet1/0/1
[5500-Ethernet1/0/1] wred 2 64 20
```

### Configuring Traffic Accounting

Refer to “Traffic-based Traffic Accounting” on page 692 for information about traffic accounting.

**Configuration prerequisites**

- The ACL rules for traffic identifying are defined. Refer to “ACL Configuration” on page 663 for information about defining ACL rules.
The port that needs this configuration is determined.

**Configuration procedure**

**Table 518  Configuring traffic accounting**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure traffic</td>
<td>traffic-statistic inbound acl-rule</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, traffic accounting is disabled.</td>
</tr>
<tr>
<td>Clear the traffic statistics</td>
<td>reset traffic-statistic inbound acl-rule</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuration example**

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Perform traffic accounting on the packets sourced from the 10.1.1.0/24 network segment.
- Clear the traffic statistics.

**Configuration procedure:**

```plaintext
<5500> system-view  
[5500] acl number 2000  
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255  
[5500-acl-basic-2000] quit  
[5500] interface Ethernet1/0/1  
[5500-Ethernet1/0/1] traffic-statistic inbound ip-group 2000  
[5500-Ethernet1/0/1] reset traffic-statistic inbound ip-group 2000
```

**Enabling the Burst Function**

Refer to “Burst” on page 692 for information about the burst function.

**Configuration prerequisites**

The burst function is required.

**Configuration procedure**

**Table 519  Enable the burst function**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable the burst function</td>
<td>burst-mode enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the burst function is disabled.</td>
</tr>
</tbody>
</table>

**Caution:** With the IRF function enabled, do not enable the burst function. Refer to the IRF Fabric part for the detailed information about IRF.

**Configuration example**

- Enable the burst function
Configuration procedure:

<5500> system-view
[5500] burst-mode enable

**Configuring Traffic Mirroring**

Refer to “Traffic mirroring” on page 692 for information about traffic mirroring.

**Configuration prerequisites**

- The ACL rules for traffic identifying are defined. Refer to “ACL Configuration” on page 663 for information about defining ACL rules.
- The source mirroring ports and mirroring direction are determined.
- The destination mirroring port is determined.

**Configuration procedure**

**Table 520  Configure traffic mirroring**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the current port as the a source mirroring port</td>
<td>Switch 5500: mirrored-to { inbound</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>outbound } acl-rule { monitor-interface</td>
<td>Omit the following steps if you redirect traffic to the CPU.</td>
</tr>
<tr>
<td></td>
<td>cpu }</td>
<td>Proceed to the following steps if you redirect traffic to a port</td>
</tr>
<tr>
<td></td>
<td>Switch 5500G: mirrored-to inbound</td>
<td></td>
</tr>
<tr>
<td></td>
<td>acl-rule { monitor-interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cpu }</td>
<td></td>
</tr>
<tr>
<td>Quit to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Configure the current port as a source mirroring port</td>
<td>In system view mirroring-group group-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>monitor-port monitor-port-id</td>
<td>Use either approach</td>
</tr>
<tr>
<td></td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>monitor-port</td>
<td></td>
</tr>
</tbody>
</table>

For information on using the `mirroring-group monitor-port` and `monitor-port` commands refer to “Configuring Traffic Mirroring” on page 704.

**Configuration example**

Network requirements:

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Duplicate the packets from network segment 10.1.1.0/24 to the destination mirroring port Ethernet 1/0/4.

Configuration procedure:

<5500> system-view
[5500] acl number 2000
[5500-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[5500-acl-basic-2000] quit
[5500] interface Ethernet1/0/4
QoS Configuration Example

Displaying and Maintaining QoS

After completing the above configuration, you can execute the `display` command in any view to view the running status of QoS and verify the configuration.

Table 521  Display QoS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the mapping between 802.1p priority and local precedence</td>
<td><code>display qos cos-local-precedence-map</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the priority marking configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } traffic-priority`</td>
</tr>
<tr>
<td>Display the protocol packet priority configuration</td>
<td><code>display protocol-priority</code></td>
<td></td>
</tr>
<tr>
<td>Display LR configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } line-rate`</td>
</tr>
<tr>
<td>Display traffic policing configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } traffic-limit`</td>
</tr>
<tr>
<td>Display traffic redirecting configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } traffic-redirect`</td>
</tr>
<tr>
<td>Display VLAN mapping configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } traffic-remark-vlanid`</td>
</tr>
<tr>
<td>Display queue scheduling configuration</td>
<td><code>display queue-scheduler</code></td>
<td></td>
</tr>
<tr>
<td>Display traffic accounting configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } traffic-statistic`</td>
</tr>
<tr>
<td>Display traffic mirroring configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } mirrored-to`</td>
</tr>
<tr>
<td>Display all the QoS configuration</td>
<td>`display qos-interface { interface-type interface-number</td>
<td>unit-id } all`</td>
</tr>
</tbody>
</table>

QoS Configuration Example

Network requirement

An enterprise network connects all the departments through an Ethernet switch. PC 1, with the IP address 192.168.0.1 belongs to the R&D department and is connected to Ethernet 1/0/1 of the switch. The marketing department is connected to Ethernet 1/0/2 of the switch.

Configure TP and LR to satisfy the following requirements:

- Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps. Drop the packets exceeding the rate limit.
Set the maximum rate of outbound IP packets sent by PC 1 in the R&D department to 640 kbps. Drop the packets exceeding the rate limit.

**Network diagram**

**Figure 206** Network diagram for TP and rate limiting configuration

Configuration procedure

1. Define an ACL for traffic identifying.

   ```
   # Create ACL 2000 and enter basic ACL view.
   <5500> system-view
   [5500] acl number 2000
   
   # Define a rule for the packets with 192.168.0.1 as the source IP address.
   [5500-acl-basic-2000] rule permit source 192.168.0.1 0
   [5500-acl-basic-2000] quit
   ```

2. Configure TP and rate limiting

   ```
   # Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps.
   [5500] interface Ethernet1/0/2
   [5500-Ethernet1/0/2] line-rate inbound 64
   [5500-Ethernet1/0/2] quit
   
   # Set the maximum rate of outbound IP packets sent by PC1 in the R&D department to 640 kbps.
   [5500] interface Ethernet1/0/1
   [5500-Ethernet1/0/1] traffic-limit inbound ip-group 2000 640 exceed drop
   ```

**Configuration Example of Priority Marking and Queue Scheduling**

**Network requirements**

An enterprise network connects all the departments through an Ethernet switch. Two clients, PC 1 and PC 2, are connected to Ethernet 1/0/1 of the switch. Server 1 (the database server), Server 2 (the mail server), and Server 3 (the file server) are connected to Ethernet 1/0/2 of the switch.
Configure priority marking and queue scheduling on the switch to enable the packets of Server 1, Server 2, and Server 3 being processed on the switch in this priority order: Server 1, Server 2, and Server 3 (in descending order).

**Network diagram**

*Figure 207*  Network diagram for priority marking and queue scheduling configuration

---

**Configuration procedure**

1. Define an ACL for traffic identifying

   # Create ACL 3000 and enter advanced ACL view.

   ```
   <5500> system-view
   [5500] acl number 3000
   
   # Define ACL rules for identifying packets based on destination IP addresses.
   [5500-acl-adv-3000] rule 0 permit ip destination 192.168.0.1 0
   [5500-acl-adv-3000] rule 1 permit ip destination 192.168.0.2 0
   [5500-acl-adv-3000] rule 2 permit ip destination 192.168.0.3 0
   [5500-acl-adv-3000] quit
   ```

2. Configure priority marking

   # Mark priority for packets received through Ethernet 1/0/1 and matching ACL 3000.

   ```
   [5500] interface Ethernet1/0/1
   [5500-Ethernet1/0/1] traffic-priority inbound ip-group 3000 rule 0 local-precedence 4
   [5500-Ethernet1/0/1] traffic-priority inbound ip-group 3000 rule 1 local-precedence 3
   [5500-Ethernet1/0/1] traffic-priority inbound ip-group 3000 rule 2 local-precedence 2
   [5500-Ethernet1/0/1] quit
   ```

3. Configure queue scheduling

   # Apply SP queue scheduling algorithm.

   ```
   [5500] queue-scheduler strict-priority
   ```
QoS Profile Configuration

Overview

Introduction to QoS Profile

A QoS profile is a set of QoS configurations. It provides an easy way for performing and managing QoS configuration. A QoS profile can contain one or multiple QoS functions. In networks where hosts change their positions frequently, you can define QoS policies for the hosts and add the QoS policies to a QoS profile. When a host is connected to another port of a switch, you can simply apply the corresponding QoS profile to the port to maintain the same QoS configuration performed for the host.

Currently, a QoS profile can contain configurations concerning packet filtering, TP, and priority marking.

QoS Profile Application Mode

Dynamic application mode

A QoS profile can be applied dynamically to a user or a group of users passing 802.1x authentication. To apply QoS profiles dynamically, a user name-to-QoS profile mapping table is required on the AAA server. For a switch operating in this mode, after a user passes the 802.1x authentication, the switch looks up the user name-to-QoS profile mapping table for the QoS profile using the user name and then applies the QoS profile found to the port the user is connected to.

Corresponding to the 802.1x authentication modes, dynamic QoS profile application can be user-based and port-based.

- User-based QoS profile application

The switch generates a new QoS profile by adding user source MAC address information to the identifying rule defined in the existing QoS profile and then applies the new QoS profile to the port the user is connected to.

- Port-based QoS profile application

The switch directly applies the QoS profile to the port the user is connected to.

A user-based QoS profile application fails if the traffic identifying rule defined in the QoS profile contains source address information (including source MAC address and source IP address information).

Manual application mode

You can use the apply command to manually apply a QoS profile to a port.
QoS Profile Configuration

Table 522  QoS profile configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a QoS Profile</td>
<td>Required</td>
<td>“Configuring a QoS Profile”</td>
</tr>
<tr>
<td>Configure to apply a QoS Profile dynamically</td>
<td>Optional</td>
<td>“Applying a QoS Profile”</td>
</tr>
<tr>
<td>Apply a QoS Profile manually</td>
<td>Optional</td>
<td>“Applying a QoS Profile”</td>
</tr>
</tbody>
</table>

Configuring a QoS Profile

Configuration prerequisites

- The ACL rules used for traffic identifying are defined. Refer to “ACL Configuration” on page 663 for information about defining ACL rules.
- The type and number of actions in the QoS profile are specified.

Configuration procedure

Table 523  Configure a QoS profile

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Create a QoS profile and enter QoS profile view</td>
<td>qos-profile profile-name</td>
<td></td>
</tr>
<tr>
<td>Configure TP</td>
<td>traffic-limit inbound acl-rule</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure packet filtering</td>
<td>Switch 5500: packet-filter { inbound</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure priority marking</td>
<td>Switch 5500G: packet-filter inbound acl-rule</td>
<td>Refer to &quot;ACL Configuration&quot; on page 663 for information about packet filtering.</td>
</tr>
</tbody>
</table>

Applying a QoS Profile

You can configure to apply a QoS profile dynamically or simply apply a QoS profile manually.
Configuration prerequisites

- To configure to apply a QoS profile dynamically, make sure 802.1x is enabled both globally and on the port, and the authentication mode is determined. For information about 802.1x, refer to “802.1x Configuration” on page 477 and “System Guard Configuration” on page 505.
- To apply a QoS profile manually, make sure the port to which the QoS profile is to be applied is determined.
- The QoS profile to be applied is determined.

Configuration procedure

Table 524 Configure to apply a QoS profile dynamically

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Specify the mode to apply a QoS profile</td>
<td>qos-profile port-based</td>
<td>Optional By default, the mode to apply a QoS profile is user-based.</td>
</tr>
<tr>
<td>Configure the mode to apply a QoS profile and port-based</td>
<td>undo qos-profile port-based</td>
<td>If the 802.1x authentication mode is MAC address-based, the mode to apply a QoS profile must be configured user-based.</td>
</tr>
<tr>
<td>Configure the mode to apply a QoS profile as user-based</td>
<td>apply qos-profile profile-name interface interface-list</td>
<td>By default, a port has no QoS profile applied to it.</td>
</tr>
</tbody>
</table>

Table 525 Apply a QoS profile manually

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Apply a QoS profile to specific ports</td>
<td>apply qos-profile profile-name interface interface-list</td>
<td>Select either of the operations. By default, a port has no QoS profile applied to it.</td>
</tr>
<tr>
<td>In system view</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a QoS profile to the current port</td>
<td>apply qos-profile profile-name</td>
<td></td>
</tr>
<tr>
<td>In Ethernet port view</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Displaying and Maintaining QoS Profile Configuration

After completing the above configuration, you can execute the display command in any view to view the running status of the QoS profile and verify the configuration.
QoS Profile Configuration Example

Network requirements
All departments of a company are interconnected through a switch. The 802.1x protocol is used to authenticate users and control their access to network resources. A user name is someone, and the authentication password is hello. It is connected to Ethernet 1/0/1 of the switch and belongs to the test.net domain.

It is required to configure a QoS profile to limit the rate of all the outbound IP packets of the user to 128 kbps and configuring to drop the packets exceeding the target packet rate.

Network diagram

<table>
<thead>
<tr>
<th>Table 526 Display QoS profile configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Display QoS profile configuration</td>
</tr>
</tbody>
</table>

Configuration procedure

1 Configuration on the AAA server

# Configure the user authentication information and the matching relationship between the user name and the QoS profile. Refer to the AAA server's documentation of the for the detailed configuration requirements.

2 Configuration on the switch

# Configure IP addresses for the RADIUS server.

<5500> system-view
[5500] radius scheme radius1
[5500-radius-radius1] primary authentication 10.11.1.1
[5500-radius-radius1] primary accounting 10.11.1.2
[5500-radius-radius1] secondary authentication 10.11.1.2
[5500-radius-radius1] secondary accounting 10.11.1.1

# Set the encryption passwords for the switch to exchange packets with the
# authentication RADIUS servers and accounting RADIUS servers.

[5500-radius-radius1] key authentication money
[5500-radius-radius1] key accounting money

# Configure the switch to delete the user domain name from the user name and
# then send the user name to the RADIUS server.

[5500-radius-radius1] user-name-format without-domain
[5500-radius-radius1] quit

# Create the user domain test.net and specify radius1 as your RADIUS server
# group.

[5500] domain test.net
[5500-isp-test.net] radius-scheme radius1
[5500-isp-test.net] quit

# Create ACL 3000 to permit IP packets destined for any IP address.

[5500] acl number 3000
[5500-acl-adv-3000] rule 1 permit ip destination any
[5500-acl-adv-3000] quit

# Define a QoS profile named example to limit the rate of matched packets to
# 128 kbps and configuring to drop the packets exceeding the target packet rate.

[5500] qos-profile example
[5500-qos-profile-example] traffic-limit inbound ip-group 3000 128 exceed drop

# Enable 802.1x.

[5500] dot1x
[5500] dot1x interface Ethernet1/0/1

After the configuration, the QoS profile named example will be applied to the
user with user name someone automatically after the user passes the
authentication.
Web Cache Redirection Overview

Usually, users access Web pages through Hypertext Transfer Protocol (HTTP). Typically, users connect to the Internet through LANs. For LANs containing large amounts of users of the Internet, HTTP traffics may congest the links between the LANs and the Internet and may even affect the operation of other services. Web cache server can relieve the HTTP load on the links connecting LANs and the Internet and improve the speed of users’ obtaining information from the Internet.

The Web cache redirection function provided by the switch 5500 can redirect the HTTP traffic to Web cache servers, as illustrated in Figure 209.

**Figure 209**  A Web cache redirection implementation

As shown in Figure 209, PC 1 and PC 2 are hosts in a LAN connected to the switch, which belong to VLAN 10 and VLAN 20 respectively. The gateway address of PC 1 is set to the IP address of VLAN-interface 10; the gateway address of PC 2 is set to the IP address of VLAN-interface 20. Web Cache Server is used to store the information from the Internet that is frequently accessed by the users in the LAN. It belongs to VLAN 30. The switch connects to the router through VLAN 40. Normally, HTTP traffic of PC 1 and PC 2 are forwarded through VLAN 40 to the router, which then sends the traffic to the Internet. By enabling Web cache redirection function on the switch, HTTP traffic of PC 1 and PC 2 is redirected to Web Cache Server through VLAN 30.

When a user in the LAN accesses the Internet,

- If the information requested is already stored in Web Cache Server, the Web Cache Server sends the information to the user directly, thus eliminating the access to the Internet.
If Web Cache Server does not contain the information requested, it retrieves the information from the Internet and then forwards the information to the user.

If both the Web cache redirection function and the STP function are configured on the switch, to avoid Web cache redirection failure, you are recommended to configure the port connecting with the Web Cache Server as a Trunk or Hybrid port that permits the packets of the VLAN used for HTTP traffic transmission, VLAN 40 in Figure 209 for example.

Web Cache Redirection Configuration

Configuration Prerequisites

- The route between the switch and the Web cache server is reachable, and the Web cache function is enabled on the Web cache server.
- The IP address and MAC address of the Web cache server and the VLANs whose HTTP traffic is to be redirected to the Web cache are configured.
- The port through which the switch is connected to the Web cache server and TCP port number used by HTTP are determined.

Configuration Procedure

You can configure Web cache redirection in system view or Ethernet port (connecting with the Web cache server) view.

Table 527 Configure Web cache redirection in system view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Configure Web cache server parameters</td>
<td><code>webcache address ip-address mac mac-address</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td><code>vlan vlan-id port interface-type interface-number [ tcpport tcpport-number ]</code></td>
<td>Not configured by default.</td>
</tr>
<tr>
<td>Specify a VLAN whose HTTP traffic is to be redirected to the Web cache server</td>
<td><code>webcache redirect-vlan vlan-id</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no HTTP packet is redirected to the Web cache server.</td>
</tr>
</tbody>
</table>

Table 528 Configure Web cache redirection in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Configure Web cache server parameters</td>
<td><code>webcache address ip-address mac mac-address</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td><code>vlan vlan-id [ tcpport tcpport-number ]</code></td>
<td>Not configured by default.</td>
</tr>
<tr>
<td>Quit to system view</td>
<td><code>quit</code></td>
<td></td>
</tr>
</tbody>
</table>
Displaying Web Cache Redirection Configuration

Make sure the route between the switch and Web cache server is reachable for the Web cache redirection function to take effect.

A switch can have only one Web cache server configured. That is, a newly configured Web cache server replaces the existing one.

Make sure both the interface of the VLAN that the Web cache server belongs to and that of the VLAN whose HTTP traffic is to be redirected are up for the Web cache redirection to take effect.

A switch does not support redirecting the VLAN HTTP traffic where the Web cache server resides to the Web cache server.

### Displaying Web Cache Redirection Configuration

After completing the above configuration, you can execute the `display` command in any view to display the operation of Web cache redirection and thus verify your configuration.

#### Table 528  Configure Web cache redirection in Ethernet port view

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a VLAN whose HTTP traffic is to be redirected to the Web cache server</td>
<td><code>webcache redirect-vlan vlan-id</code></td>
<td>Required By default, no HTTP packet is redirected to the Web cache server.</td>
</tr>
</tbody>
</table>

#### Networking requirements

The network of a company is organized as follows.

- The market department belongs to VLAN 10 and is connected to port Ethernet 1/0/1 of the switch. The IP address of VLAN 10 interface is 192.168.1.1/24.

- The R&D department belongs to VLAN 20 and is connected to port Ethernet 1/0/2 of the switch. The IP address of VLAN 20 interface is 192.168.2.1/24.

- The administrative department belongs to VLAN 30 and is connected to port Ethernet 1/0/3 of the switch. The IP address of VLAN 30 interface is 192.168.3.1/24.

- The WEB Cache Server, with the IP address 192.168.4.2 and the MAC address 0012-0990-2250, belongs to VLAN 40 and is connected to port Ethernet 1/0/4 of the switch. The IP address of VLAN 40 interface is 192.168.4.1/24.

---

**Table 529  Display Web cache redirection**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Web cache redirection configuration and the status of the Web cache</td>
<td><code>display webcache</code></td>
<td>Available in any view.</td>
</tr>
</tbody>
</table>
The switch is connected to the router through port Ethernet 1/0/5 and accesses the Internet through the router. Ethernet 1/0/5 belongs to VLAN 50. The IP address of VLAN 50 interface is 192.168.5.1/24.

The WEB Cache redirection function is enabled on the switch, and all the packets of the market department, R&D department, and administrative department are redirected to the WEB Cache Server, so as to relieve the load from the connection links of the WAN, and improve the speed of Internet access.

Networking diagram

Figure 210  Networking diagram for Web cache redirection configuration

Configuration procedure

# Create VLAN 10 for the market department, and assign an IP address 192.168.1.1 to the VLAN-interface 10.

```
<5500> system-view
[5500] vlan 10
[5500-vlan10] port Ethernet 1/0/1
[5500-vlan10] quit
[5500] interface Vlan-interface 10
[5500-Vlan-interface10] ip address 192.168.1.1 24
[5500-Vlan-interface10] quit
```

# Create VLAN 20 for the R&D department, and assign an IP address 192.168.2.1 to the VLAN-interface 20.

```
[5500] vlan 20
[5500-vlan20] port Ethernet 1/0/2
[5500-vlan20] quit
[5500] interface Vlan-interface 20
```
Web Cache Redirection Configuration Example

[5500-Vlan-interface20] ip address 192.168.2.1 24
[5500-Vlan-interface20] quit

# Create VLAN 30 for the administrative department, and assign an IP address 192.168.3.1 to the VLAN-interface 30.

[5500] vlan 30
[5500-vlan30] port Ethernet 1/0/3
[5500-vlan30] quit
[5500] interface Vlan-interface 30
[5500-Vlan-interface30] ip address 192.168.3.1 24
[5500-Vlan-interface30] quit

# Create VLAN 40 for the WEB Cache Server, and assign an IP address 192.168.4.1 to the VLAN-interface 40.

[5500] vlan 40
[5500-vlan40] port Ethernet 1/0/4
[5500-vlan40] quit
[5500] interface Vlan-interface 40
[5500-Vlan-interface40] ip address 192.168.4.1 24
[5500-Vlan-interface40] quit

# Create VLAN 50 for the switch to connect to the router, and assign an IP address 192.168.5.1 to VLAN-interface 50.

[5500] vlan 50
[5500-vlan50] port Ethernet 1/0/5
[5500-vlan50] quit
[5500] interface Vlan-interface 50
[5500-Vlan-interface50] ip address 192.168.5.1 24
[5500-Vlan-interface50] quit

# Configure port Ethernet 1/0/4 (through which the switch connects to the Web Cache Server) as a Truck port, and configure the port to allow the packets of VLAN 40 and VLAN 50 to pass through.

[5500] interface Ethernet 1/0/4
[5500-Ethernet1/0/4] port link-type trunk
[5500-Ethernet1/0/4] port trunk permit vlan 40 50
[5500-Ethernet1/0/4] quit

# Enable the WEB Cache redirection function, and redirect all the HTTP packets received on VLAN 10, VLAN 20 and VLAN 30 to the WEB Cache Server.

[5500] webcache address 192.168.4.2 mac 0012-0990-2250 vlan 40 port Ethernet 1/0/4
[5500] webcache redirect-vlan 10
[5500] webcache redirect-vlan 20
[5500] webcache redirect-vlan 30
Mirroring Overview

Mirroring occurs when packets are duplicated from a port to another port connected with a data monitoring device for network monitoring and diagnosis. The port where packets are duplicated is called the source mirroring port or the monitored port and the port to which duplicated packets are sent is called the destination mirroring port or the monitor port as shown in Figure 211.

![Figure 211 Mirroring](image)

The Switch 5500 supports three types of port mirroring:

- **Local Port Mirroring**
- **Remote Port Mirroring**
- **Traffic Mirroring**

They are described in the following sections.

**Local Port Mirroring**

In local port mirroring, packets passing through one or more source ports of a device are copied to the destination port on the same device for packet analysis and monitoring. In this case, the source ports and the destination port must be located on the same device.

**Remote Port Mirroring**

Remote port mirroring does not require the source and destination ports to be on the same device. The source and destination ports can be located on multiple devices across the network. This allows an administrator to monitor the traffic on remote devices conveniently.
To implement remote port mirroring, a special VLAN, called a remote-probe VLAN, is used. All mirrored packets are sent from the reflector port of the source switch to the monitor port (destination port) on the destination switch through the remote-probe VLAN. Figure 212 illustrates the implementation of remote port mirroring.

**Figure 212** Remote port mirroring application

The switches involved in the remote port mirroring implementation play the following three roles.

- **Source switch**: The source switch is the device where the monitored port is located. It copies traffic passing through the monitored port to the reflector port. The reflector port then transmits the traffic to an intermediate switch (if any) or destination switch through the remote-probe VLAN.

- **Intermediate switch**: The intermediate switch switches between the source switch and destination switch on the network. An intermediate switch forwards mirrored traffic flows to the next intermediate switch or the destination switch through the remote-probe VLAN. No intermediate switch is present if the source and destination switches directly connect to each other.

- **Destination switch**: The destination switch is where the monitor port is located. The destination switch forwards the mirrored traffic flows it received from the remote-probe VLAN to the monitoring device through the destination port.

Table 530 describes how the ports on various switches are involved in the mirroring operation.

**Table 530** Ports involved in the mirroring operation

<table>
<thead>
<tr>
<th>Switch</th>
<th>Ports involved</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source switch</td>
<td>Source port</td>
<td>Port monitored. It copies packets to the reflector port through local port mirroring. There can be more than one source port.</td>
</tr>
<tr>
<td></td>
<td>Reflector port</td>
<td>Receives packets from the source port and broadcasts the packets in the remote-probe VLAN.</td>
</tr>
<tr>
<td></td>
<td>Trunk port</td>
<td>Sends mirrored packets to the intermediate switch or the destination switch.</td>
</tr>
</tbody>
</table>
### Configuring Mirroring

<table>
<thead>
<tr>
<th>Switch</th>
<th>Ports involved</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermediate switch</td>
<td>Trunk port</td>
<td>Sends mirrored packets to the destination switch. Two trunk ports are necessary for the intermediate switch to connect the devices at the source switch side and the destination switch side.</td>
</tr>
<tr>
<td>Destination switch</td>
<td>Trunk port</td>
<td>Receives remote mirrored packets.</td>
</tr>
<tr>
<td></td>
<td>Destination port</td>
<td>Receives packets forwarded from the trunk port and transmits the packets to the data detection device.</td>
</tr>
</tbody>
</table>

**CAUTION:**
- Do not configure a default VLAN, a management VLAN, or a dynamic VLAN as the remote-probe VLAN.
- Configure all ports connecting the devices in the remote-probe VLAN as trunk ports, and ensure the Layer 2 connectivity from the source switch to the destination switch over the remote-probe VLAN.
- Do not configure a Layer 3 interface for the remote-probe VLAN, run other protocol packets, or carry other service packets on the remote-probe VLAN and do not use the remote-probe VLAN as the voice VLAN and protocol VLAN; otherwise, remote port mirroring may be affected.

**Traffic Mirroring**
Traffic mirroring uses ACL to monitor traffic that matches certain criteria on a specific port. Unlike port mirroring where all inbound and outbound traffic passing through a port is monitored, traffic mirroring provides a finer monitoring granularity. For detailed configuration information about traffic mirroring, refer to “QoS Profile Configuration” on page 709.

**Configuring Mirroring**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring Local Port Mirroring”</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Remote Port Mirroring&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>

- On a Switch 5500, only one destination port for local port mirroring or one reflector port for remote port mirroring can be configured, and the two kinds of ports cannot both exist.
- When you mirror packets sent by ports on an expansion module, the packets from a port on the front panel to the expansion module cannot be mirrored if the monitor port is not on the expansion module. Refer to the installation manual for the introduction to the front panel and expansion module.
Configuring Local Port Mirroring

**Configuration prerequisites**
- The source port is determined and the direction in which the packets are to be mirrored is determined.
- The destination port is determined.

**Configuration procedure**

**Table 532  Configure port mirroring on the switch 5500**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a port mirroring group</td>
<td>mirroring-group group-id local</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the source port for the port mirroring group</td>
<td>In system view mirroring-group group-id mirroring-port mirroring-port-list { both</td>
<td>Use either approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inbound</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mirroring-group group-id mirroring-port { both</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quit</td>
</tr>
<tr>
<td>Configure the destination port for the port mirroring group</td>
<td>In system view mirroring-group group-id monitor-port monitor-port-id interface interface-type interface-number</td>
<td>Use either approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In port view mirroring-group group-id monitor-port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When configuring local port mirroring, note that:

- You need to configure the source and destination ports for the local port mirroring to take effect.
- The source port and the destination port cannot be a fabric port or a member port of an existing mirroring group; besides, the destination port cannot be a member port of an aggregation group or a port enabled with LACP or STP.

Configuring Remote Port Mirroring

The Switch 5500 can serve as a source switch, an intermediate switch, or a destination switch in a remote port mirroring networking environment.

**Configuration on a switch acting as a source switch**

1 **Configuration prerequisites**
   - The source port, the refector port, and the remote-probe VLAN are determined.
   - Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.
   - The direction of the packets to be monitored is determined.

2 **Configuration procedure**
Table 533  Configuration on the source switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a VLAN and enter the VLAN view</td>
<td>vlan vlan-id</td>
<td>vlan-id is the ID of the remote-probe VLAN.</td>
</tr>
<tr>
<td>Configure the current VLAN as the remote-probe VLAN</td>
<td>remote-probe vlan enable</td>
<td>Required</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Enter the view of the Ethernet port that connects to the intermediate switch or destination switch</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the current port as trunk port</td>
<td>port link-type trunk</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the port type is Access.</td>
</tr>
<tr>
<td>Configure the trunk port to permit packets from the remote-probe VLAN</td>
<td>port trunk permit vlan remote-probe-vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Create a remote source mirroring group</td>
<td>mirroring-group group-id remote-source</td>
<td>Required</td>
</tr>
<tr>
<td>Configure source port(s) for the remote source mirroring group</td>
<td>mirroring-group group-id mirroring-port mirroring-port-list { both</td>
<td>inbound</td>
</tr>
<tr>
<td>Configure the reflector port for the remote source mirroring group</td>
<td>mirroring-group group-id reflector-port reflector-port</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the remote-probe VLAN for the remote source mirroring group</td>
<td>mirroring-group group-id remote-probe vlan remote-probe-vlan-id</td>
<td>Required</td>
</tr>
</tbody>
</table>

When configuring the source switch, note that:

- All ports of a remote source mirroring group are on the same device. Each remote source mirroring group can be configured with only one reflector port.
- The reflector port cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP. It must be an access port and cannot be configured with functions like VLAN-VPN, port loopback detection, packet filtering, QoS, and port security.
- You cannot modify the duplex mode, port rate, and MDI attribute of a reflector port.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- Do not configure a port connecting the intermediate switch or destination switch as the mirroring source port. Otherwise, traffic disorder may occur in the network.
**Configuration on a switch acting as an intermediate switch**

1 Configuration prerequisites
   - The trunk ports and the remote-probe VLAN are determined.
   - Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2 Configuration procedure

<table>
<thead>
<tr>
<th>Table 534</th>
<th>Configuration on the intermediate switch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>Create a VLAN and enter VLAN view</td>
<td><strong>vlan vlan-id</strong></td>
</tr>
<tr>
<td>Configure the current VLAN as the remote-probe VLAN</td>
<td><strong>remote-probe vlan enable</strong></td>
</tr>
<tr>
<td>Return to system view</td>
<td><strong>quit</strong></td>
</tr>
<tr>
<td>Enter the view of the Ethernet port connecting to the source switch, destination switch or other intermediate switch</td>
<td><strong>interface interface-type interface-number</strong></td>
</tr>
<tr>
<td>Configure the current port as trunk port</td>
<td><strong>port link-type trunk</strong></td>
</tr>
<tr>
<td>Configure the trunk port to permit packets from the remote-probe VLAN</td>
<td><strong>port trunk permit vlan remote-probe-vlan-id</strong></td>
</tr>
</tbody>
</table>

*The Switch 5500 acting as the intermediate switch in remote port mirroring networking does not support bidirectional packet mirroring (the both keyword).*

**Configuration on a switch acting as a destination switch**

1 Configuration prerequisites
   - The destination port and the remote-probe VLAN are determined.
   - Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2 Configuration procedure

<table>
<thead>
<tr>
<th>Table 535</th>
<th>Configure remote port mirroring on the destination switch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>Create a VLAN and enter VLAN view</td>
<td><strong>vlan vlan-id</strong></td>
</tr>
<tr>
<td>Configure the current VLAN as a remote-probe VLAN</td>
<td><strong>remote-probe vlan enable</strong></td>
</tr>
<tr>
<td>Return to system view</td>
<td><strong>quit</strong></td>
</tr>
<tr>
<td>Enter the view of the Ethernet port connecting to the source switch or an intermediate switch</td>
<td><strong>interface interface-type interface-number</strong></td>
</tr>
</tbody>
</table>
When configuring a destination switch, note that:

- The destination port of remote port mirroring cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.

### Displaying and Maintaining Port Mirroring

After completing the above configuration, you can execute the `display` commands in any view to view the mirroring running information, so as to verify your configurations.

### Table 536 Display mirroring configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the port mirroring configuration</td>
<td>`display mirroring-group { group-id</td>
<td>all</td>
</tr>
</tbody>
</table>

### Local Port Mirroring Configuration Example

**Network requirements**

The departments of a company connect to each other through the Switch 5500:

- Research and Development (R&D) department is connected to Switch C through Ethernet 1/0/1.
- Marketing department is connected to Switch C through Ethernet 1/0/2.
- Data detection device is connected to Switch C through Ethernet 1/0/3
The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure Ethernet 1/0/1 and Ethernet 1/0/2 as mirroring source ports.
- Configure Ethernet 1/0/3 as the mirroring destination port.

**Network diagram**

*Figure 213  Network diagram for local port mirroring*

**Configuration procedure**

Configure Switch C:

# Create a local mirroring group.

```
<5500> system-view
[5500] mirroring-group 1 local
```

# Configure the source ports and destination port for the local mirroring group.

```
[5500] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 both
[5500] mirroring-group 1 monitor-port Ethernet 1/0/3
```

# Display configuration information about local mirroring group 1.

```
[5500] display mirroring-group 1
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    Ethernet1/0/1 both
    Ethernet1/0/2 both
  monitor port: Ethernet1/0/3
```

After the configurations, you can monitor all packets received on and sent from the R&D department and the marketing department on the data detection device.
Remote Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through Switch 5500s:
- Switch A, Switch B, and Switch C are Switch 5500s.
- Department 1 is connected to Ethernet 1/0/1 of Switch A.
- Department 2 is connected to Ethernet 1/0/2 of Switch A.
- Ethernet 1/0/3 of Switch A connects to Ethernet 1/0/1 of Switch B.
- Ethernet 1/0/2 of Switch B connects to Ethernet 1/0/1 of Switch C.
- The data detection device is connected to Ethernet 1/0/2 of Switch C.

The administrator wants to monitor the packets sent from Department 1 and 2 through the data detection device.

Use the remote port mirroring function to meet the requirement. Perform the following configurations:

- Use Switch A as the source switch, Switch B as the intermediate switch, and Switch C as the destination switch.
- On Switch A, create a remote source mirroring group, configure VLAN 10 as the remote-probe VLAN, ports Ethernet 1/0/1 and Ethernet 1/0/2 as the source ports, and port Ethernet 1/0/4 as the reflector port.
- On Switch B, configure VLAN 10 as the remote-probe VLAN.
- Configure Ethernet 1/0/3 of Switch A, Ethernet 1/0/1 and Ethernet 1/0/2 of Switch B, and Ethernet 1/0/1 of Switch C as trunk ports, allowing packets of VLAN 10 to pass.
- On Switch C, create a remote destination mirroring group, configure VLAN 10 as the remote-probe VLAN, and configure Ethernet 1/0/2 connected with the data detection device as the destination port.

Network diagram

Figure 214  Network diagram for remote port mirroring

Configuration procedure

1. Configure the source switch (Switch A)

   # Create remote source mirroring group 1.
# Configure VLAN 10 as the remote-probe VLAN.

```
<5500> system-view
[5500] mirroring-group 1 remote-source
```

# Configure VLAN 10 as the remote-probe VLAN.

```
[5500] vlan 10
[5500-vlan10] remote-probe vlan enable
[5500-vlan10] quit
```

# Configure the source ports, reflector port, and remote-probe VLAN for the remote source mirroring group.

```
[5500] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 inbound
[5500] mirroring-group 1 reflector-port Ethernet 1/0/4
[5500] mirroring-group 1 remote-probe vlan 10
```

# Configure Ethernet 1/0/3 as trunk port, allowing packets of VLAN 10 to pass.

```
[5500] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] port link-type trunk
[5500-Ethernet1/0/3] port trunk permit vlan 10
[5500-Ethernet1/0/3] quit
```

# Display configuration information about remote source mirroring group 1.

```
[5500] display mirroring-group 1
mirroring-group 1:
  type: remote-source
  status: active
  mirroring port:
    Ethernet1/0/1 inbound
    Ethernet1/0/2 inbound
  reflector port: Ethernet1/0/4
  remote-probe vlan: 10
```

2 Configure the intermediate switch (Switch B)

# Configure VLAN 10 as the remote-probe VLAN.

```
<5500> system-view
[5500] vlan 10
[5500-vlan10] remote-probe vlan enable
[5500-vlan10] quit
```

# Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] port link-type trunk
[5500-Ethernet1/0/1] port trunk permit vlan 10
[5500-Ethernet1/0/1] quit
```

# Configure Ethernet 1/0/2 as the trunk port, allowing packets of VLAN 10 to pass.

```
[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port link-type trunk
[5500-Ethernet1/0/2] port trunk permit vlan 10
```
3 Configure the destination switch (Switch C)

# Create remote destination mirroring group 1.

<5500> system-view
[5500] mirroring-group 1 remote-destination

# Configure VLAN 10 as the remote-probe VLAN.

[5500] vlan 10
[5500-vlan10] remote-probe vlan enable
[5500-vlan10] quit

# Configure the destination port and remote-probe VLAN for the remote destination mirroring group.

[5500] mirroring-group 1 monitor-port Ethernet 1/0/2
[5500] mirroring-group 1 remote-probe vlan 10

# Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] port link-type trunk
[5500-Ethernet1/0/1] port trunk permit vlan 10
[5500-Ethernet1/0/1] quit

# Display configuration information about remote destination mirroring group 1.

[5500] display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: Ethernet1/0/2
    remote-probe vlan: 10

After the configurations, you can monitor all packets sent from Department 1 and 2 on the data detection device.
Intelligent resiliency framework (IRF), which is specific to the Switch 5500 and Switch 5500G, is a new technology for building the network core. This feature allows you to build an IRF fabric by interconnecting several Switch 5500s or 5500Gs to provide more ports for network devices and improve the reliability of your networks.

This section describes an IRF fabric on the Switch 5500. For a description of an IRF fabric on the Switch 5500G, see “An IRF Fabric on the Switch 5500G” on page 744.

Establishing an IRF Fabric

Topological and IRF fabric connections

An IRF fabric typically has a ring topology. As shown in Figure 215, each switch has two ports connected with two other switches in the fabric. These two ports are called fabric ports in general, a left port and a right port respectively. The other ports, which are available for connections with users or devices outside of the fabric, are called user ports.

Figure 215  A schematic diagram of an IRF fabric

A correctly build IRF fabric features the following:

- Multiple Switch 5500s are interconnected through their fabric ports.
- The switch’s left port is connected to the right port of another switch and its right port is connected to the left port of a third one.

As shown in Figure 216, IRF fabric also supports bus topology, which has the same requirements as the ring topology. The difference is that each of the switches
across the bus connection is connected with the other switches through only one fabric port.

**Figure 216** Network diagram for IRF fabric with a bus topology

![Network diagram for IRF fabric with a bus topology](image)

**Fabric ports**

On a Switch 5500, only four GigabitEthernet ports can be configured as fabric ports. The four ports fall into two groups according to their port number:

- GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 form the first group.
- GigabitEthernet 1/1/3 and GigabitEthernet 1/1/4 form the second group.

Only one group of ports can be configured as fabric ports at a time. Given a group, either GigabitEthernet 1/1/1 or GigabitEthernet 1/1/3 can be configured as the left fabric port, and either GigabitEthernet 1/1/2 or GigabitEthernet 1/1/4 can be configured as the right fabric port.

Once you configure a port as a fabric port, the group that comprises this fabric port becomes the fabric port group, and you cannot configure a port in the other group as a fabric port. For example, once you configure GigabitEthernet 1/1/1 as a fabric port, this port automatically becomes the left port and the first group becomes the fabric port group.

*The system does not require a consistency in the fabric port groups between different switches. That is, the left fabric port in the first group of a switch can be connected to the right fabric port in the second group of the peer switch.*

**FTM**

As the basis of the IRF function, the Fabric Topology Management (FTM) program manages and maintains the entire topology of a fabric.

With fabric ports configured, the FTM program releases device information of the device through the fabric ports. The device information includes Unit ID, CPU MAC, device type ID, fabric port information, and all fabric configuration information. The device information is released in the discovery packet (DISC).

After receiving the packet, the peer device will analyze the packet. A device can form a fabric with the peer or join a fabric only when the following conditions are met.
The number of the existing devices in the fabric does not reach the maximum number of devices allowed by the fabric (up to eight devices can form a fabric.).

The fabric name of the device and the existing devices in the fabric are the same.

The software version of the device is the same as that of the existing devices in the fabric.

The device passes the security authentication if security authentication is enabled on the device or in the fabric, that is, the same authentication mode and password are configured on the device and the existing devices in the fabric.

In case IRF automatic fabric is enabled, even if the software version of the local device is inconsistent with that used on the device in the fabric, you can still add a device to the fabric by automatic downloading and loading of the software.

**IRF fabric detection**

Forming a fabric requires a high consistency of connection modes between the devices and device information. Without all the requirements for forming a fabric being met, a fabric cannot be formed.

The FTM program detects the necessary conditions for forming a fabric one by one and displays the detection results. You can use the `display ftm information` command to view the detection information for the fabric, checking the running status of the fabric or analyzing the problems. Table 537 lists the status and solution of the problems.

**Table 537  Status and solution**

<table>
<thead>
<tr>
<th>Status</th>
<th>Analysis</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>-</td>
<td>These three kinds of information do not mean a device or a fabric operates improperly. No measure is needed for any of them.</td>
</tr>
<tr>
<td>temporary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>redundancy port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection error</td>
<td>Indicates three kinds of port matching errors may occur.</td>
<td>Pull out one end of the cable and connect it to a fabric port of another switch.</td>
</tr>
<tr>
<td></td>
<td>Two fabric ports of the same device (that is, the right port and the left port) are connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The left and right fabric ports of the devices are not connected in a crossed way.</td>
<td>Connect the left and right ports of two devices in a crossed way.</td>
</tr>
<tr>
<td></td>
<td>A fabric port of the local switch is connected to a non-fabric port, or is connected to a fabric port that does not have fabric port function enabled.</td>
<td>Check the types of the two interconnected ports on two sides. Make sure a fabric port is only connected to ports of the same type and the fabric ports on both sides are enabled with the fabric port function.</td>
</tr>
</tbody>
</table>
CHAPTER 63: IRF FABRIC CONFIGURATION

IRF automatic fabric

If the software version and fabric name of the local device are inconsistent with those of the device in the IRF fabric, the local device cannot be added to the fabric. In this case, you have to manually download and load the software, and then restart the device, or manually change the fabric name to add the device to the fabric. 3Com Switch 5500s provide the IRF automatic fabric function, which enables the device to automatically download the software and change the fabric name, thus reducing the manual maintenance workload.

With IRF automatic fabric enabled, if inconsistency in software version or fabric name occurs when a switch is added to a fabric, the system automatically performs the following operations:

- If the software version of the local device is inconsistent with that of the device in the fabric, the system automatically initiates a download request to the device with the smallest unit ID in the fabric and downloads the software used by the device in the current fabric to the local device. Then the device will automatically restart and be added to the fabric.

- If the fabric name of the local device is inconsistent with that of the device in the fabric, the system automatically ignores the inconsistency check of the fabric name and adds the device to the fabric. Then the system automatically synchronizes the configurations to the device with the smallest unit ID and changes the fabric name.

With the above operations completed, the device can be added to the fabric and work normally.

Caution:

- You need to enable the IRF automatic fabric function on all the devices including the newly added device in the fabric to enable the newly added device to download software and discovery neighbors and thus be added to the fabric normally.
3Com recommends that you set the Unit ID of the switch with the software to be downloaded to 1, and thus ensure that the candidate switch can download a correct software version.

How IRF Works

When a fabric is established, the devices determine their respective roles in the fabric by comparing their CPU MAC addresses. The device with the lowest CPU MAC address is elected as the master and the other devices are slaves.

After the election, the fabric can operate normally. The following three functions of IRF can provide simple configuration mode, enhanced network performance and perfect redundancy backup mechanism for users.

- The Switch 5500 supports enhanced IRF fabric features, including Distributed Device Management (DDM), Distributed Redundancy Routing (DRR), and Distributed Link Aggregation (DLA)

DDM

DDM is a new device management mode provided by IRF. In normal cases, a fabric can be considered as a single device. You can manage the entire fabric by logging onto any device in the fabric with different logging modes. The devices in the fabric synchronize their configurations by exchanging packets, thus ensuring stability of the fabric.

FTM program uses Unit ID, or device ID to distinguish between the devices in a fabric when you manage them. On initialization of the IRF function, each device considers its Unit ID as 1 and after a fabric connection is established, the FTM program automatically re-numbers the devices or you can manually configure the Unit ID of them.

The master in a fabric collects the newest configurations of the user and the slaves periodically synchronize the configurations from the master. In this way, the entire fabric can operate with the same configurations.

DRR

DRR is used to implement redundancy routing backup. The devices in a fabric run their independent routing protocols and maintain their own routing tables. Unlike a common layer 3 switch, a fabric member does not generate a layer 3 forwarding table to forward packets, instead, it uploads the routing table to the master, which generates a forwarding table used by the entire fabric by integrating the routing tables of all the devices. Then each slave synchronizes this forwarding table from the master and takes it as the basis for layer 3 forwarding.

In this way, the forwarding table entries of each device in the fabric can be consistent. Even if the master fails, other devices can use the forwarding table synchronized from the master to perform layer 3 forwarding, thus ensuring the accuracy of forwarding path. After re-electing the master, the fabric will restart routing update.

DLA

As a new link aggregation mode, DLA can improve fault tolerance and redundancy backup of user networks.
Link aggregation enables you to configure ports on the same device as an aggregation port group, avoiding network interruptions resulted from single port failure. Based on link aggregation, DLA provides a more reliable solution, with which you can select ports on different devices to form an aggregation port group. In this way, single port failure can be avoided and network reliability can be greatly improved, because the fabric can communicate with the destination network through ports on other devices in case a single device fails.

### Configuring an IRF Fabric on the Switch 5500

This section describes how to configure an IRF fabric on the Switch 5500. For a description of an IRF Fabric on the Switch 5500G, see “Configuring an IRF Fabric on the Switch 5500G” on page 749.

### IRF Fabric Configuration Tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the Fabric Port of a Switch</td>
<td>Required</td>
<td>“Specifying the Fabric Port of a Switch”</td>
</tr>
<tr>
<td>Specifying the VLAN Used to Form an IRF Fabric</td>
<td>Optional</td>
<td>“Specifying the VLAN Used to Form an IRF Fabric”</td>
</tr>
<tr>
<td>Setting a Unit ID for a Switch</td>
<td>Optional</td>
<td>“Setting a Unit ID for a Switch”</td>
</tr>
<tr>
<td>Assigning a Unit Name to a Switch</td>
<td>Optional</td>
<td>“Assigning a Unit Name to a Switch”</td>
</tr>
<tr>
<td>Assigning an IRF Fabric Name to a Switch</td>
<td>Optional</td>
<td>“Assigning an IRF Fabric Name to a Switch”</td>
</tr>
<tr>
<td>Setting the IRF Fabric Authentication Mode</td>
<td>Optional</td>
<td>“Setting the IRF Fabric Authentication Mode”</td>
</tr>
</tbody>
</table>

### Specifying the Fabric Port of a Switch

You can specify the fabric port of a switch in either system view or Ethernet interface view.

#### Configuration tasks in system view

Follow the steps in Table 539 to configure a fabric in system view.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the fabric port of a switch</td>
<td>fabric-port interface-type interface-number enable</td>
<td>Required. Not specified by default</td>
</tr>
</tbody>
</table>

#### Configurations in Ethernet interface view

Follow the steps in Table 539 to configure a fabric in Ethernet interface view.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet interface view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
</tbody>
</table>
Establishing an IRF system requires a high consistency of the configuration of each device. Hence, before you enable the fabric port, do not perform any configuration for the port, and do not configure some functions that affect the IRF (such as TACACS and VLAN-VPN) for other ports or globally. Otherwise, you cannot enable the fabric port. For detailed restrictions refer to the error information output by the devices.

After an IRF fabric is established successfully, do not enable the burst function on any device within the IRF Fabric. For introduction to the burst function, refer to the QoS&QoS Profile part of the manual.

When you have enabled fabric port function for a fabric port group, if you need to change the fabric port group, you must disable the fabric function of the current fabric port group before you configure another group. Otherwise, the system will prompt that the current fabric port group is in use, you cannot change the fabric port group.

As shutting down a fabric port directly may cause the fabric to be split and error messages, do not perform such operations.

To split a fabric, you can simply remove the cables used to form the fabric or disable the fabric using the undo fabric-port enable command.

You can shut down/bring up a port after you disable the fabric feature on the port.

If you need to configure an IRF fabric as a DHCP server, configure the UDP Helper function in the fabric at the same time to ensure that the client can successfully obtain an IP address. Since this configuration can be automatically synchronized to the entire fabric you can perform it on only one unit. For the configuration of the UDP Helper function, refer to “UDP Helper Configuration” on page 791.

After you use the port link-type irf-fabric command to specify a port as the fabric port, you cannot use the port link-type command to change the port to a port of other types. You must use the undo fabric-port command first to disable the fabric port function of the port to change the port type.

### Specifying the VLAN Used to Form an IRF Fabric

When the devices in an IRF fabric are transmitting IRF data, to avoid it being sent to other non fabric ports, the data should be transmitted in a specified VLAN. You can specify the VLAN used to transmit IRF data.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the VLAN used to form the IRF</td>
<td>ftm fabric-vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the VLAN used to form</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the IRF fabric is VLAN 4093</td>
</tr>
</tbody>
</table>

### Specifying the VLAN Used to Transmit IRF Data

When the devices in an IRF fabric are transmitting IRF data, to avoid it being sent to other non fabric ports, the data should be transmitted in a specified VLAN. You can specify the VLAN used to transmit IRF data.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the VLAN used to form the IRF</td>
<td>ftm fabric-vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the VLAN used to form</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the IRF fabric is VLAN 4093</td>
</tr>
</tbody>
</table>
CAUTION: You cannot specify an existing VLAN to form an IRF fabric; otherwise, your configuration fails.

Setting a Unit ID for a Switch

On the switches that support automatic numbering, FTM will automatically number the switches to constitute an IRF fabric by default, so that each switch has a unique unit ID in the fabric. You can use the command in the following table to set unit IDs for switches. Make sure to set different unit IDs for different switches in an IRF fabric. Otherwise, FTM will automatically number the switches with the same unit ID.

Table 542 Set a unit ID for a switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set a unit ID for the switch</td>
<td>change self-unit to { unit-id</td>
<td>auto-numbering }</td>
</tr>
</tbody>
</table>

If you do not configure the fabric port, you cannot change the unit ID of the local switch.

After an IRF fabric is established, you can use the following command to change the unit IDs of the switches in the IRF fabric.

Table 543 Set a unit ID to a new value

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set a unit ID to a new value</td>
<td>change unit-id unit-id1 to { unit-id2</td>
<td>auto-numbering }</td>
</tr>
</tbody>
</table>

- Unit IDs in an IRF fabric are not always arranged in order of 1 to 8.
- Unit IDs of an IRF fabric can be inconsecutive.

After you change the unit ID of switches, the following operations are performed.

- If the modified unit ID does not exist in the IRF fabric, the system sets its priority to 5 and saves it in the unit Flash memory.

- If the modified unit ID is an existing one, the system prompt you to confirm if you really want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. Then you can use the fabric save-unit-id command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

- If auto-numbering is selected, the system sets the unit priority to 10. You can use the fabric save-unit-id command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

Priority is the reference for FTM program to perform automatic numbering. The value of priority can be 5 or 10. Priority 5 means the switch adopts manual...
numbering, and priority 10 means the switch adopts automatic numbering. Manual numbering has a higher priority than automatic numbering.

After the configuration of numbering, you can use the following command in the table to save the local unit ID in the unit Flash memory. When you restart the switch, it can load the unit ID configuration automatically.

**Table 544** Save the unit ID of each unit in the IRF fabric

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the unit ID of each unit in the IRF fabric</td>
<td><code>fabric save-unit-id</code></td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Assigning a Unit Name to a Switch**

You can assign a unit name to a switch by performing the operations listed in Table 545.

**Table 545** Assign a unit name to a switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Assign a unit name to a switch</td>
<td><code>set unit unit-id name unit-name</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

**Assigning an IRF Fabric Name to a Switch**

Only the switches with the same IRF fabric name can form an IRF fabric.

**Table 546** Assign a fabric name to a switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Assign a fabric name to the switch</td>
<td><code>sysname sysname</code></td>
<td>Optional</td>
</tr>
<tr>
<td>By default, the IRF fabric name is 5500.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Setting the IRF Fabric Authentication Mode**

Only the switches with the same IRF fabric authentication mode can form an IRF fabric.

**Table 547** Set the IRF fabric authentication mode for a switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Set the IRF fabric authentication mode for the switch</td>
<td>`irf-fabric authentication-mode { simple password</td>
<td>md5 key }`</td>
</tr>
<tr>
<td>By default, no authentication mode is set on a switch.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When an IRF fabric operates normally, you can regard the whole fabric as a single device and perform configuration on it. Multiple switches constitute an IRF fabric. Therefore, data transmission and simultaneous program execution among the switches may cause the IRF fabric in a busy situation. When you configure the IRF fabric, you may receive a prompt **Fabric system is busy, please try later...** which indicates the fabric system does not perform your configuration properly. In this case, you need to verify your previous configuration or perform your configuration again.
1.2.8 Configuring IRF Automatic Fabric for a Switch

I. Configuration prerequisites

Make sure that the Flash of the newly added device has enough space to download software used on the device in the fabric.

Configure the fabric port for the newly added device.

Configuration procedure

Follow the steps in Table 548 to configure IRF automatic fabric for a switch.

Table 548  Configure IRF automatic fabric for a switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure IRF automatic fabric for a switch</td>
<td>fabric member-auto-update</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>software enable</td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

Caution:

- You need to enable the IRF automatic fabric function on all the devices including the newly added device in the fabric to enable the newly added device to download software and discovery neighbors and thus be added to the fabric normally.

- After you configure the IRF automatic fabric function on Slave, execute the save command to save the configurations as soon as possible. Otherwise, the device may synchronize the configurations from Master and restart repeatedly because the configurations on the device are lost after the device automatically downloads the software and restarts.

Displaying and Maintaining IRF Fabric for the Switch 5500

This section describes how to display and maintain an IRF fabric on the Switch 5500. For instructions on displaying and maintaining an IRF fabric on the Switch 5500G, see “Displaying and Maintaining IRF Fabric for the Switch 5500G” on page 752.

After completing the configuration in the previous sections, you can execute the display command in any view to view device management and verify the settings. And you can execute the reset command to clear the FTM statistics.

Table 549  Display and maintain FTM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the topology information of an IRF fabric</td>
<td>display ftm {information topology-database}</td>
<td></td>
</tr>
<tr>
<td>Clear the FTM statistics</td>
<td>reset ftm statistics</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>
Switch 5500 IRF Fabric Configuration Example

This section provides an IRF configuration example for the Switch 5500. For an example of an IRF configuration on the Switch 5500G, see “Switch 5500G IRF Fabric Configuration Example” on page 753.

Network Requirements

Configure unit ID, unit name, IRF fabric name, and authentication mode for four switches to enable them to form an IRF fabric as shown in Figure 217.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello
- Authentication mode: simple password
- Password: welcome

Network Diagram

Figure 217 Network diagram for forming an IRF fabric

Configuration Procedure

1 Configure Switch A.

   # Configure fabric ports.

   <5500> system-view
   [5500] fabric-port GigabitEthernet1/1/1 enable

   [5500] fabric-port GigabitEthernet1/1/2 enable

   # Configure the unit name as Unit 1.

   [5500] set unit 1 name Unit1

   # Configure the fabric name as hello.

   [5500] sysname hello
# Configure the fabric authentication mode as `simple` and the password as `welcome`.

```
[hello] irf-fabric authentication-mode simple welcome
```

2 Configure Switch B.

# Configure fabric ports.

```
<5500> system-view
[5500] fabric-port GigabitEthernet1/1/1 enable
[5500] fabric-port GigabitEthernet1/1/2 enable
```

# Set the unit ID to 2.

```
[5500] change unit-id 1 to 2
```

# Configure the unit name as `Unit 2`.

```
[5500] set unit 1 name unit2
```

# Configure the fabric name as `hello`.

```
[5500] sysname hello
```

# Configure the fabric authentication mode as `simple` and the password as `welcome`.

```
[hello] irf-fabric authentication-mode simple welcome
```

Configurations on Switch C and Switch D are similar with the above configurations.

---

**An IRF Fabric on the Switch 5500G**

This section describes an IRF fabric on the Switch 5500G. For a description of an IRF Fabric on the Switch 5500, see “An IRF Fabric on the Switch 5500” on page 733.

**Establishing an IRF Fabric**

An IRF fabric typically has a ring topology structure. As shown in Figure 218, each Switch 5500G uses two special ports on the rear panel to connect with two other switches in the fabric. The two ports are called fabric ports in general, UP port and DOWN port respectively; the other ports of the switch, which are available for connections with users or devices outside the fabric, are called user ports.
A correctly built IRF fabric features the following:

- Multiple Switch 5500Gs are interconnected through their fabric ports.
- Given a switch, its UP port is connected to the DOWN port of another switch, and its DOWN port is connected to the UP port of a third one.

The port connection mode for the Switch 5500G ring topology for an IRF fabric is shown in Figure 219.

IRF fabric also supports bus topology, which has the same requirements as the ring topology. The difference is that each of the switches across the bus connection is connected with the other switches through only one fabric port, as shown in Figure 220.
**Fabric ports**

On a Switch 5500G, only the two cascade ports on its rear panel can be configured as the fabric ports. The two cascade ports are:

- **UP port**: Cascade 1/2/1
- **DOWN port**: Cascade 1/2/2

**FTM**

As the basis of the IRF function, the Fabric Topology Management (FTM) program manages and maintains the entire topology of a fabric.

With fabric ports configured, the FTM program releases device information of the device through the fabric ports. The device information includes Unit ID, CPU MAC, device type ID, fabric port information, and all fabric configuration information. The device information is released in the discovery packet (DISC).

After receiving the packet, the peer device will analyze the packet. A device can form a fabric with the peer or join a fabric only when the following conditions are met.

- The number of the existing devices in the fabric does not reach the maximum number of devices allowed by the fabric (up to eight devices can form a fabric).
- The fabric name of the device and the existing devices in the fabric are the same.
- The software version of the device is the same as that of the existing devices in the fabric.

In case IRF automatic fabric is enabled, even if the software version of the local device is inconsistent with that used on the device in the fabric, you can still add a device to the fabric by automatic downloading and loading of the software.

**IRF fabric detection**

Forming a fabric requires a high consistency of connection modes between the devices and device information. Without all the requirements for forming a fabric being met, a fabric cannot be formed.

The FTM program detects the necessary conditions for forming a fabric one by one and displays the detection results. You can use the `display ftm information` command to view the detection information for the fabric, checking the running
status of the fabric or analyzing the problems. Table 550 lists the status and solution to the problems.

Table 550  Status and solution

<table>
<thead>
<tr>
<th>Status</th>
<th>Analysis</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td></td>
<td>These three kinds of information do not mean a device or a fabric operates improperly. No measure is needed for any of them.</td>
</tr>
<tr>
<td>temporary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>redundancy port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection error</td>
<td>Indicates three kinds of port matching errors may occur.</td>
<td>Pull out one end of the cable and connect it to a fabric port of another switch.</td>
</tr>
<tr>
<td></td>
<td>Two fabric ports of the same device (that is, the UP port and the DOWN port) are connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The UP and DOWN fabric ports of the devices are not connected in a crossed way.</td>
<td>Connect the up and DOWN ports of two devices in a crossed way.</td>
</tr>
<tr>
<td></td>
<td>A fabric port of the local switch is connected to a fabric port that does not have fabric port function enabled.</td>
<td>Make sure that the fabric ports on both sides are enabled with the fabric port function.</td>
</tr>
<tr>
<td>reached max units</td>
<td>The maximum number of units allowed by the current fabric is reached. You will fail to add new devices to the fabric in this case.</td>
<td>Remove the new device or existing devices in the fabric.</td>
</tr>
<tr>
<td>different system name</td>
<td>The fabric name of the device directly connected to the switch and the existing fabric name of the fabric are not the same.</td>
<td>Modify the fabric name of the new device to be that of the fabric.</td>
</tr>
<tr>
<td>different product version</td>
<td>The software version of the directly connected device and that of the current device are not the same.</td>
<td>Update the software version to make sure the software version of the new device is the same as that of the fabric.</td>
</tr>
</tbody>
</table>

IRF automatic fabric

If the software version and fabric name of the local device are inconsistent with those of the device in the IRF fabric, the local device cannot be added to the fabric. In this case, you have to manually download and load the software, and then restart the device, or manually change the fabric name to add the device to the fabric. 3Com Switch 5500Gs provide the IRF automatic fabric function, which enables the device to automatically download the software and change the fabric name, thus reducing the manual maintenance workload.

With IRF automatic fabric enabled, if inconsistency in software version or fabric name occurs when a switch is added to a fabric, the system automatically performs the following operations:
If the software version of the local device is inconsistent with that of the device in the fabric, the system automatically initiates a download request to the device with the smallest unit ID in the fabric and downloads the software used by the device in the current fabric to the local device. Then the device will automatically restart and be added to the fabric.

If the fabric name of the local device is inconsistent with that of the device in the fabric, the system automatically ignores the inconsistency check of the fabric name and adds the device to the fabric. Then the system automatically synchronizes the configurations to the device with the smallest unit ID and changes the fabric name.

With the above operations completed, the device can be added to the fabric and work normally.

**Caution:**

- You need to enable the IRF automatic fabric function on all the devices including the newly added device in the fabric to enable the newly added device to download software and discovery neighbors and thus be added to the fabric normally.

- 3Com recommends that you set the Unit ID of the switch with the software to be downloaded to 1, and thus ensure that the candidate switch can download the correct software version.

**How IRF Works**

When a fabric is established, the devices determine their respective roles in the fabric by comparing their CPU MAC addresses. The device with the lowest CPU MAC address is elected as the master and the other devices are slaves.

After the election, the fabric can operate normally. The following three functions of IRF can provide simple configuration mode, enhanced network performance and perfect redundancy backup mechanism for users.

**DDM**

Distributed Device Management (DDM) is a new device management mode provided by IRF. In normal cases, a fabric can be considered as a single device. You can manage the entire fabric by logging onto any device in the fabric with different logging modes. The devices in the fabric synchronize their configurations by exchanging packets, thus ensuring stability of the fabric.

FTM program uses Unit ID, or device ID to distinguish between the devices in a fabric when you manage them. On initialization of the IRF function, each device considers its Unit ID as 1 and after a fabric connection is established, the FTM program automatically re-numbers the devices or you can manually configure the Unit ID of them.

The master in a fabric collects the newest configurations of the user and the slaves periodically synchronize the configurations from the master. In this way, the entire fabric can operate with the same configurations.

**DRR**

Distributed Redundancy Routing (DRR) is used to implement redundancy routing backup. The devices in a fabric run their independent routing protocols and
maintain their own routing tables. Unlike a common layer 3 switch, a fabric member does not generate a layer 3 forwarding table to forward packets; instead, it uploads the routing table to the master, which generates a forwarding table used by the entire fabric by integrating the routing tables of all the devices. Then each slave synchronizes this forwarding table from the master and takes it as the basis for layer 3 forwarding.

In this way, the forwarding table entries of each device in the fabric can be consistent. Even if the master fails, other devices can use the forwarding table synchronized from the master to perform layer 3 forwarding, thus ensuring the accuracy of forwarding path. After re-electing the master, the fabric will restart routing update.

**DLA**

As a new link aggregation mode, Distributed Link Aggregation (DLA) can improve fault tolerance and redundancy backup of user networks.

Link aggregation enables you to configure ports on the same device as an aggregation port group, avoiding network interruptions resulted from single port failure. Based on link aggregation, DLA provides a more reliable solution, with which you can select ports on different devices to form an aggregation port group. In this way, single port failure can be avoided and network reliability can be greatly improved, because the fabric can communicate with the destination network through ports on other devices in case a single device fails.

---

**Configuring an IRF Fabric Configuration on the Switch 5500G**

This section describes how to configure an IRF fabric on the Switch 5500G. For a description of an IRF Fabric on the Switch 5500, see “Configuring an IRF Fabric Configuration on the Switch 5500” on page 738.

**IRF Fabric Configuration Task List**

Complete the tasks in to configure IRF fabric:

**Table 551**

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the Fabric Port of a Switch</td>
<td>Required</td>
</tr>
<tr>
<td>Setting a Unit ID for a Switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Assigning a Unit Name to a Switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Assigning an IRF Fabric Name to a Switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring IRF Automatic Fabric for a Switch</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Specifying the Fabric Port of a Switch**

Follow these steps to specify a fabric port:

**Table 552**  Specifying the Fabric Port of a Switch

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the fabric port of a switch</td>
<td>fabric-port interface-type interface-number enable</td>
<td>Required</td>
</tr>
</tbody>
</table>

Not specified by default
Establishing an IRF system requires a high consistency of the configuration of each device. Hence, before you enable the fabric port, do not perform any configuration for the port, and do not configure some functions that affect the IRF (such as TACACS and VLAN-VPN) for other ports or globally. Otherwise, you cannot enable the fabric port. For detailed restrictions refer to the error information output by devices.

After an IRF fabric is established successfully, do not enable the burst function on any device within the IRF Fabric. For introduction to the burst function, refer to the QoS&QoS Profile part of the manual.

To split a fabric, you can simply remove the cables used to form the fabric or disable the fabric using the `undo fabric-port enable` command.

If you need to configure an IRF fabric as a DHCP server, configure the UDP Helper function in the fabric at the same time to ensure that the client can successfully obtain an IP address. (Since this configuration can be automatically synchronized to the entire fabric, you can perform it on only one unit.) For the configuration of the UDP Helper function, refer to the UDP Helper part of this manual.

Setting a Unit ID for a Switch

On the switches that support automatic numbering, FTM will automatically number the switches to constitute an IRF fabric by default, so that each switch has a unique unit ID in the fabric. You can use the command in the following table to set unit IDs for switches. Make sure to set different unit IDs for different switches in an IRF fabric. Otherwise, FTM will automatically number the switches with the same unit ID.

Follow the steps in Table 553 to set a unit ID for a switch:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
| Set a unit ID for the switch | change self-unit to {unit-id | auto-numbering} | Optional By default, the unit ID of a switch that belongs to no IRF fabric is 1. The unit ID of a switch belonging to an IRF fabric is assigned by FTM. Unit ID ranges from 1 to 8.

If you do not enable the fabric port, you cannot change the unit ID of the local switch.

After an IRF fabric is established, you can use the following command to change the unit IDs of the switches in the IRF fabric.

Follow the steps in Table 554 to set a unit ID to a new value:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set a unit ID to a new value</td>
<td>change unit-id unit-id1 to {unit-id2</td>
<td>auto-numbering}</td>
</tr>
</tbody>
</table>
- Unit IDs in an IRF fabric are not always arranged in order of 1 to 8.
- Unit IDs of an IRF fabric can be inconsecutive.

After you change the unit ID of switches, the following operations are performed.

- If the modified unit ID does not exist in the IRF fabric, the system sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit ID is an existing one, the system prompts you to confirm if you really want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. Then you can use the fabric save-unit-id command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.
- If auto-numbering is selected, the system sets the unit priority to 10. You can use the fabric save-unit-id command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

Priority is the reference for FTM program to perform automatic numbering. The value of priority can be 5 or 10. Priority 5 means the switch adopts manual numbering, and priority 10 means the switch adopts automatic numbering. Manual numbering has a higher priority than automatic numbering.

After the configuration of numbering, you can use the following command in the table to save the local unit ID in the unit Flash memory. When you restart the switch, it can load the unit ID configuration automatically.

Follow the steps in Table 555 to save the unit ID of each unit in the IRF fabric:

### Table 555 Saving the unit ID of each unit in the IRF fabric

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the unit ID of each unit in the IRF fabric</td>
<td>fabric save-unit-id</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Assigning a Unit Name to a Switch**

Follow the steps in Table 556 to assign a unit name to a switch:

### Table 556 Assigning a Unit Name to a Switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Assign a unit name to a switch</td>
<td>set unit-id name unit-name</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Assigning an IRF Fabric Name to a Switch**

Only the switches with the same IRF fabric name can form an IRF fabric.

Follow the steps in Table 557 to assign a fabric name to a switch:

### Table 557 Assigning an IRF Fabric Name to a Switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Assign a fabric name to the switch</td>
<td>sysname</td>
<td>Optional</td>
</tr>
</tbody>
</table>

By default, the IRF fabric name is 3Com.
CHAPTER 63: IRF FABRIC CONFIGURATION

Configuring IRF Automatic Fabric for a Switch

Configuration prerequisites

- Make sure that the Flash of the newly added device has enough space to download software used on the device in the fabric.
- Configure the fabric port for the newly added device.

Configuration procedure

Follow the steps in Table 558 to configure IRF automatic fabric for a switch:

Table 558 Configuring IRF Automatic Fabric for a Switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure IRF automatic fabric</td>
<td>fabric member-auto-update</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>software enable</td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

Caution:

- You need to enable the IRF automatic fabric function on all the devices including the newly added device in the fabric to enable the newly added device to download software and discovery neighbors and thus be added to the fabric normally.
- After you configure the IRF automatic fabric function on Slave, execute the save command to save the configurations as soon as possible. Otherwise, the device may synchronize the configurations from Master and restart repeatedly because the configurations on the device are lost after the device automatically downloads the software and restarts.

When fabric works normally, you can configure the whole fabric as an individual device. As a fabric is comprised of multiple devices, busy working state may occur due to data transmission between devices or synchronous execution of programs. When you perform an operation, if you receive a prompt "Fabric system is busy, please try later…!", which indicates that the fabric does not execute your configuration properly, you need to verify your configuration or reconfigure the previous operation.

Displaying and Maintaining IRF Fabric for the Switch 5500G

This section describes how to display and maintain an IRF fabric on the Switch 5500G. For instructions on displaying and maintaining an IRF fabric on the Switch 5500, see “Displaying and Maintaining IRF Fabric for the Switch 5500” on page 742.

After completing the configuration in the previous sections, you can execute the display command in any view to view device management and verify the settings. And you can execute the reset command to clear the FTM statistics.
This section provides an IRF configuration example for the Switch 5500G. For an example of an IRF configuration on the Switch 5500, see “Switch 5500 IRF Fabric Configuration Example” on page 743.

Network Requirements
Configure unit ID, unit name, and IRF fabric name for four switches to enable them to form an IRF fabric as shown in Figure 1-3.

The configuration details are as follows:
- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello

Network Diagram

Figure 221  Network diagram for forming an IRF fabric

Configuration Procedure

1) Configure Switch A.

# Configure fabric ports.

<5500G> system-view
[5500G] fabric-port Cascade 1/2/1 enable
[5500G] fabric-port Cascade 1/2/2 enable

# Configure the unit name as Unit 1.

Table 559  Display and maintain FTM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the topology information of an IRF fabric</td>
<td>display ftm { information</td>
<td>topology-database }</td>
</tr>
<tr>
<td>Clear the FTM statistics</td>
<td>reset ftm statistics</td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>
[5500G] set unit 1 name Unit1

# Configure the fabric name as hello.
[5500G] sysname hello

2) Configure Switch B.

# Configure fabric ports.

<5500G> system-view
[5500G] fabric-port Cascade 1/2/1 enable
[5500G] fabric-port Cascade 1/2/2 enable

# Set the unit ID to 2.
[5500G] change unit-id 2 to 2

# Configure the unit name as Unit 2.
[5500G] set unit 1 name unit2

# Configure the fabric name as hello.

[5500G] sysname hello

Configurations on Switch C and Switch D are similar with the above configurations.
Cluster Overview

Introduction to Switch Clustering

A cluster contains a group of switches. Through cluster management, you can manage multiple geographically dispersed in a centralized way.

Cluster management is implemented through 3Com’s Switch Clustering feature. A switch in a cluster plays one of the following three roles:

- Management device
- Member device
- Candidate device

A cluster comprises of a management device and multiple member devices. To manage the devices in a cluster, you need only to configure an external IP address for the management switch. Cluster management enables you to configure and manage remote devices in batches, reducing the workload of the network configuration. Normally, there is no need to configure external IP addresses for member devices. Figure 222 illustrates a cluster implementation.

Figure 222  A cluster implementation
Switch Clustering has the following advantages:

- It eases the configuration and management of multiple switches: You just need to configure a public IP address for the management device instead of for all the devices in the cluster; and then you can configure and manage all the member devices through the management device without the need to log onto them one by one.
- It provides the topology discovery and display function, which assists in monitoring and maintaining the network.
- It allows you to configure and upgrade multiple switches at the same time.
- It enables you to manage your remotely devices conveniently regardless of network topology and physical distance.
- It saves IP address resource.

**Roles in a Cluster**

The switches in a cluster play different roles according to their functions and status. You can specify the role a switch plays. A switch in a cluster can also switch to other roles under specific conditions.

As mentioned above, the three cluster roles are management device, member device, and candidate device.

**Table 560 Description of cluster roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Configuration</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management device</td>
<td>Configured with a external IP address</td>
<td>- Provides an interface for managing all the switches in a cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Manages member devices through command redirection, that is, it forwards the commands intended for specific member devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Discovers neighbors, collects the information about network topology, manages and maintains the cluster. Management device also supports FTP server and SNMP host proxy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Processes the commands issued by users through the public network</td>
</tr>
<tr>
<td>Member device</td>
<td>Normally, a member device is not assigned an external IP address</td>
<td>- Members of a cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Discovers the information about its neighbors, processes the commands forwarded by the management device, and reports log. The member devices of a cluster are under the management of the management device.</td>
</tr>
</tbody>
</table>
Table 560 Description of cluster roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Configuration</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Candidate device</td>
<td>Normally, a candidate device is not assigned an external IP address</td>
<td>Candidate device refers to the devices that do not belong to any clusters but are cluster-capable.</td>
</tr>
</tbody>
</table>

Figure 223 illustrates the state machine of cluster role.

**Figure 223** State machine of cluster role

- A candidate device becomes a management device when you create a cluster on it. Note that a cluster must have one (and only one) management device. On becoming a management device, the device collects network topology information and tries to discover and determine candidate devices, which can then be added to the cluster through configurations.

- 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.

- A management device becomes a candidate device only after the cluster is removed.

After you create a cluster on a Switch 5500, the switch collects the network topology information periodically and adds the candidate switches it finds to the cluster. The interval for a management device to collect network topology information is determined by the NTDP timer. If you do not want the candidate switches to be added to a cluster automatically, you can set the topology collection interval to 0 by using the `ntdp timer` command. In this case, the switch does not collect network topology information periodically.

**How a Cluster Works**

Switch Clustering 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/maintenance of a cluster. Topology information collection and cluster establishment/maintenance are independent from each other. The former, as described below, starts before a cluster is established.

- All devices use NDP to collect the information about their neighbors, including software version, host name, MAC address, and port name.
- The management device uses NTDP to collect the information about the devices within specific hops and the topology information about the devices. It also determines the candidate devices according to the information collected.
- The management device adds the candidate devices to the cluster or removes member devices from the cluster according to the candidate device information collected through NTDP.

**Introduction to NDP**

NDP is a protocol used to discover adjacent devices and provide information about them. NDP operates on the data link layer, and therefore it supports different network layer protocols.

NDP is able to discover directly connected neighbors and provide the following neighbor information: device type, software/hardware version, and connecting port. In addition, it may provide the following neighbor information: device ID, port full/half duplex mode, product version, the Boot ROM version and so on.

- An NDP-enabled device maintains an NDP neighbor table. Each entry in the NDP table can automatically ages out. You can also clear the current NDP information manually to have neighbor information collected again.
- An NDP-enabled device regularly broadcasts NDP packet through all its active ports. An NDP packet carries a holdtime field, which indicates how long the receiving devices will keep the NDP packet data. The receiving devices store the information carried in the NDP packet into the NDP table but do not forward the NDP packet. When they receive another NDP packet, if the information carried in the packet is different from the stored one, the corresponding entry in the NDP table is updated, otherwise only the holdtime of the entry is updated.

**Introduction to NTDP**

NTDP is a protocol used to collect network topology information. NTDP provides information required for cluster management: it collects topology information about the switches within the specified hop count, so as to provide the information of which devices can be added to a cluster.

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 each device 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, and the management device triggers its NTDP to perform specific topology collection, so that its NTDP can discover topology changes timely.

The management device collects the topology information periodically. You can also launch an operation of topology information collection by executing related commands. The process of topology information collection is as follows.

- The management device sends NTDP topology collection requests periodically through its NTDP-enabled ports.
- Upon receiving an NTDP topology collection request, the device returns a NTDP topology collection response to the management device and forwards the request to its neighbor devices through its NTDP-enable ports. The topology collection response packet contains the information about the local device and the NDP information about all the neighbor devices.
- The neighbor devices perform the same operation until the NTDP topology collection request is propagated to all the devices within the specified hops.

When an NTDP topology collection request is propagated in the network, it is received and forwarded by large numbers of network devices, which may cause network congestion and the management device busy processing of the NTDP topology collection responses. To avoid such cases, the following methods can be used to control the NTDP topology collection request advertisement speed.

- Configuring the devices not to forward the NTDP topology collection request immediately after they receive an NTDP topology collection request. That is, configure the devices to wait for a period before they forward the NTDP topology collection request.
- Configuring each NTDP-enabled port on a device to forward an NTDP topology collection request after a specific period since the previous port on the device forwards the NTDP topology collection request.

- To implement NTDP, you need to enable NTDP both globally and on specific ports on the management device, and configure NTDP parameters.
- On member/candidate devices, you only need to enable NTDP globally and on specific ports.
- Member and candidate devices adopt the NTDP settings of the management device.

**Introduction to Cluster**

A cluster must have one and only one management device. Note the following when creating a cluster:

- You need to designate a management device for the cluster. The management device of a cluster is the portal of the cluster. That is, any operations from outside the network intended for the member devices of the cluster, such as accessing, configuring, managing, and monitoring, can only be implemented through the management device.
- The management device of the cluster recognizes and controls all the member devices in the cluster, no matter where they are located in the network and how they are connected.
The management device collects topology information about all member/candidate devices to provide useful information for you to establish the cluster.

By collecting NDP/NTDP information, the management device learns network topology, so as to manage and monitor network devices.

Before performing any cluster-related configuration task, you need to enable the cluster function first.

On the management device, you need to enable the cluster function and configure cluster parameters. On the member/candidate devices, however, you only need to enable the cluster function so that they can be managed by the management device.

Cluster maintenance

1 Adding a candidate device to a cluster

To create a cluster, you need to determine the device to operate as the management device first. The management device discovers and determines candidate devices through NDP and NTDP, and adds them to the cluster. You can also add candidate devices to a cluster manually.

After a candidate device is added to a cluster, the management device assigns a member number and a private IP address (used for cluster management) to it.

2 Communications within a cluster

In a cluster, the management device maintains the connections to the member devices through handshake packets. Figure 224 illustrates the state machine of the connection between the management device and a member device.

Figure 224  State machine of the connection between the management device and a member device

- After a cluster is created and a candidate device is added to the cluster as a member device, both the management device and the member device store the state information of the member device and mark the member device as Active.
- The management device and the member devices exchange handshake packets periodically. Note that the handshake packets exchanged keep the states of the member devices to be Active and are not responded.
- If the management device does not receive a handshake packet from a member device after a period three times of the interval to send handshake packets, the disconnect state is recovered.
- State holdtime exceeds the specified value.
- Fails to receive handshake packets in three consecutive intervals.
- Receives the handshake or management packets.
- Disconnect state is recovered.
- Connect
- Active
- Disconnect
packets, it changes the state of the member device from Active to Connect. Likewise, if a member device fails to receive a handshake packet from the management device after a period three times of the interval to send handshake packets, the state of the member device will also be changed from Active to Connect.

- If the management device receives a handshake packet or management packet from a member device that is in Connect state within the information holdtime, it changes the state of the member device to Active; otherwise, it changes the state of the member device (in Connect state) to Disconnect, in which case the management device considers the member device disconnected. Likewise, if this member device, which is in Connect state, receives a handshake packet or management packet from the management device within the information holdtime, it changes its state to Active; otherwise, it changes its state to Disconnect.

- If the connection between the management device and a member device in Disconnect state is recovered, the member device will be added to the cluster again. After that, the state of the member device will turn to Active both locally and on the management device.

Besides, handshake packets are also used by member devices to inform the management device of topology changes.

Additionally, on the management device, you can configure the FTP server, TFTP server, logging host and SNMP host to be shared by the whole cluster. When a member device in the cluster communicates with an external server, the member device first transmits data to the management device, which then forwards the data to the external server. The management device is the default shared FTP/TFTP server for the cluster; it serves as the shared FTP/TFTP server when no shared FTP/TFTP server is configured for the cluster.

**Management VLAN**

Management VLAN limits the range of cluster management. Through management VLAN configuration, the following functions can be implemented:

- Enabling the management packets (including NDP packets, NTDP packets, and handshake packets) to be transmitted in the management VLAN only, through which the management packets are isolated from other packets and network security is improved.

- Enabling the management device and the member devices to communicate with each other in the management VLAN.

Cluster management requires the packets of the management VLAN be permitted on ports connecting the management device and the member/candidate devices. Therefore:

- If the packets of management VLAN are not permitted on a candidate device port connecting to the management device, the candidate device cannot be added to the cluster. In this case, you can enable the packets of the management VLAN to be permitted on the port through the management VLAN auto-negotiation function.

- Packets of the management VLAN can be exchanged between the management device and a member device/candidate device without carrying
VLAN tags only when the default VLAN ID of both the two ports connecting the management device and the member/candidate device is the management VLAN. If the VLAN IDs of the both sides are not that of the management VLAN, packets of the management VLAN need to be tagged.

- **By default, the management VLAN interface is used as the network management interface.**
- **There is only one network management interface on a management device; any newly configured network management interface will overwrite the old one.**

### Tracing a device in a cluster

By tracing a device in a cluster, you can:

- Determine whether there is a loop in the cluster
- Locate which port on which switch initiates a network attack
- Determine the port and switch that a MAC address corresponds to
- Locate which switch in the cluster has a fault
- Check whether a link in the cluster and the devices on the link comply with the original plan

You can use the `tracer` command to trace a device in the cluster by specifying a destination MAC address or IP address.

The procedures are as follows:

1. **Determine whether the destination MAC address or destination IP address is used to trace a device in the cluster**
   - If you use the `tracer` command to trace the device by its MAC address, the switch will query its MAC address table according to the MAC address and VLAN ID in the command to find out the port connected with the downstream switch.
   - If you use the `tracer` command to trace the device by its IP address, the switch will query the corresponding ARP entry of the IP address to find out the corresponding MAC address and VLAN ID, and thus find out the port connected with the downstream switch.

2. **After finding out which port is connected to the downstream switch, the switch sends a multicast packet with the VLAN ID and specified hops to the port. Upon receiving the packet, the downstream switch compares its own MAC address with the destination MAC address carried in the multicast packet:**
   - If the two MAC addresses are the same, the downstream switch sends a response to the switch sending the tracer command, indicating the success of the tracer command.
   - If the two MAC addresses are different, the downstream switch will query the port connected with its downstream switch based on the MAC address and VLAN ID, and then forward the packet to its downstream switch. If within the specified hops, a switch with the specified destination MAC address is found, this switch sends a response to the switch sending the tracer command, indicating the success of the tracer command. If no switch with the
specified destination MAC address (or IP address) is found, the multicast packet will not be forwarded to the downstream any more.

- If the queried IP address has a corresponding ARP entry, but the MAC address entry corresponding to the IP address does not exist, the trace of the device fails.
- To trace a specific device using the tracemac command, make sure that all the devices passed support the tracemac function.
- To trace a specific device in a management VLAN using the tracemac command, make sure that all the devices passed are within the same management VLAN as the device to be traced.

Cluster Configuration Tasks

Before configuring a cluster, you need to determine the roles and functions the switches play. You also need to configure the related functions, preparing for the communication between devices within the cluster.

Table 561  Cluster configuration tasks:

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Configuring the Management Device&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring Member Devices&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Managing a Cluster through the Management Device&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the Enhanced Cluster Features&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Management device configuration tasks

Table 562  Management device configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NDP globally and on specific ports</td>
<td>Required</td>
<td>“Enabling NDP globally and on specific ports”</td>
</tr>
<tr>
<td>Configure NDP-related parameters</td>
<td>Optional</td>
<td>“Configuring NDP-related parameters”</td>
</tr>
<tr>
<td>Enable NTDP globally and on a specific port</td>
<td>Required</td>
<td>“Enabling NTDP globally and on a specific port”</td>
</tr>
<tr>
<td>Configure NTDP-related parameters</td>
<td>Optional</td>
<td>“Configuring NTDP-related parameters”</td>
</tr>
<tr>
<td>Enable the cluster function</td>
<td>Required</td>
<td>“Enabling the cluster function”</td>
</tr>
<tr>
<td>Configure cluster parameters</td>
<td>Required</td>
<td>“Configuring cluster parameters”</td>
</tr>
<tr>
<td>Configure interaction for the cluster</td>
<td>Optional</td>
<td>“Configuring inside-outside interaction for a cluster”</td>
</tr>
<tr>
<td>Configure NM interface for the cluster</td>
<td>Optional</td>
<td>“Configuring the network management interface for a cluster”</td>
</tr>
</tbody>
</table>

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 5500 provides the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On the management device, the preceding functions are implemented as follows:

- When you create a cluster by using the `build` or `auto-build` command, UDP port 40000 is opened at the same time.
- When you remove a cluster by using the `undo build` or `undo cluster enable` command, UDP port 40000 is closed at the same time.

### Enabling NDP globally and on specific ports

<table>
<thead>
<tr>
<th>Table 563</th>
<th>Enable NDP globally and on specific ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enable NDP globally</td>
<td><code>ndp enable</code></td>
</tr>
<tr>
<td>Enable NDP on specified Ethernet ports</td>
<td><code>ndp enable interface port-list</code></td>
</tr>
<tr>
<td>In system view</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>In Ethernet port view</td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>

### Configuring NDP-related parameters

<table>
<thead>
<tr>
<th>Table 564</th>
<th>Configure NDP-related parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Configure the holdtime of NDP information</td>
<td><code>ndp timer aging aging-in-seconds</code></td>
</tr>
<tr>
<td>Configure the interval to send NDP packets</td>
<td><code>ndp timer hello seconds</code></td>
</tr>
</tbody>
</table>

### Enabling NTDP globally and on a specific port

<table>
<thead>
<tr>
<th>Table 565</th>
<th>Enable NTDP globally and on a specific port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enable NTDP globally</td>
<td><code>ntdp enable</code></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>Enable NTDP on the Ethernet port</td>
<td><code>ntdp enable</code></td>
</tr>
<tr>
<td>Enable NTDP on the Ethernet port</td>
<td><code>ntdp enable</code></td>
</tr>
</tbody>
</table>
Configuring NTDP-related parameters

Table 566  Configure NTDP-related parameters

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the range to collect topology information</td>
<td>ntdp hop hop-value</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the device forward delay of topology collection requests</td>
<td>ntdp timer hop-delay time</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the port forward delay of topology collection requests</td>
<td>ntdp timer port-delay time</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the interval to collect topology information periodically</td>
<td>ntdp timer interval-in-minutes</td>
<td>Optional</td>
</tr>
<tr>
<td>Quit system view</td>
<td>quit</td>
<td>-</td>
</tr>
<tr>
<td>Launch topology information collection manually</td>
<td>ntdp explore</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Enabling the cluster function

Table 567  Enable the cluster function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the cluster function globally</td>
<td>cluster enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the cluster function is enabled.</td>
</tr>
</tbody>
</table>

Configuring cluster parameters

You can establish a cluster and the related configuration in manual mode or automatic mode, as described below.

- To establish a cluster and configure the cluster parameters in manual mode, perform the operations in Table 568.

Table 568  Establish a cluster and configure cluster parameters in manual mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify the management VLAN</td>
<td>management-vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, VLAN 1 is used as the management VLAN.</td>
</tr>
<tr>
<td>Enter cluster view</td>
<td>cluster</td>
<td>-</td>
</tr>
<tr>
<td>Configure a IP address pool for the cluster</td>
<td>ip-pool administrator-ip-address { ip-mask</td>
<td>ip-mask-length }</td>
</tr>
<tr>
<td>Build a cluster</td>
<td>build name</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name: cluster name.</td>
</tr>
</tbody>
</table>
To establishing a cluster in automatic mode perform the operations in Table 569.

**Table 569 Establish a cluster in automatic mode**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a multicast MAC address for the cluster</td>
<td>cluster-mac $H-H-H$</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the cluster multicast MAC address is 0180-C200-000A.</td>
</tr>
<tr>
<td>Set the interval for the management device to send multicast packets</td>
<td>cluster-mac syn-interval time-interval</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the interval to send multicast packets is one minute.</td>
</tr>
<tr>
<td>Set the holdtime of member switches</td>
<td>holdtime seconds</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the holdtime is 60 seconds.</td>
</tr>
<tr>
<td>Set the interval to send handshake packets</td>
<td>timer interval</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the interval to send handshake packets is 10 seconds.</td>
</tr>
</tbody>
</table>

After a cluster is established automatically, ACL 3998 and ACL 3999 will be generated automatically.

After a cluster is established automatically, ACL 3998 and ACL 3999 can neither be modified nor removed.

**Configuring inside-outside interaction for a cluster**

**Table 570 Configure inside-outside interaction for a cluster**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a shared FTP server for the cluster</td>
<td>ftp-server $ip-address$</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the management device acts as the shared FTP server.</td>
</tr>
<tr>
<td>Configure a shared TFTP server for the cluster</td>
<td>tftp-server $ip-address$</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no shared TFTP server is configured.</td>
</tr>
</tbody>
</table>
Cluster Configuration Tasks

1 Configuration prerequisites

- The cluster switches are properly connected;
- The shared servers are properly connected to the management switch.

2 Configuration procedure

Table 570  Configure inside-outside interaction for a cluster

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a shared logging host for the cluster</td>
<td>logging-host ip-address</td>
<td>Optional By default, no shared logging host is configured.</td>
</tr>
<tr>
<td>Configure a shared SNMP host for the cluster</td>
<td>snmp-host ip-address</td>
<td>Optional By default, no shared SNMP host is configured.</td>
</tr>
</tbody>
</table>

Configuring the network management interface for a cluster

1 Configuration prerequisites

- The cluster switches are properly connected;
- The shared servers are properly connected to the management switch.

2 Configuration procedure

Table 571  Configure the network management interface for a cluster

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter cluster view</td>
<td>cluster</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the network management (NM) interface for the cluster</td>
<td>nm-interface Vlan-interface vlan-id</td>
<td>Required By default, the management VLAN interface is used as the NM interface.</td>
</tr>
</tbody>
</table>

Member device configuration tasks

Table 572  Member device configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NDP globally and on specific ports</td>
<td>Required</td>
<td>“Enabling NDP globally and on specific ports”</td>
</tr>
<tr>
<td>Enable NTDP globally and on a specific port</td>
<td>Required</td>
<td>“Enabling NTDP globally and on a specific port”</td>
</tr>
<tr>
<td>Enable the cluster function</td>
<td>Required</td>
<td>“Enabling the cluster function”</td>
</tr>
<tr>
<td>Access shared FTP/TFTP server from a member device</td>
<td>Optional</td>
<td>“Accessing the shared FTP/TFTP server from a member device”</td>
</tr>
</tbody>
</table>

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 5500 provides the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On member devices, the preceding functions are implemented as follows:
When you execute the **add-member** command on the management device to add a candidate device to a cluster, the candidate device changes to a member device and its UDP port 40000 is opened at the same time.

When you execute the **auto-build** command on the management device to have the system automatically add candidate devices to a cluster, the candidate devices change to member devices and their UDP port 40000 is opened at the same time.

When you execute the **administrator-address** command on a device, the device's UDP port 40000 is opened at the same time.

When you execute the **delete-member** command on the management device to remove a member device from a cluster, the member device's UDP port 40000 is closed at the same time.

When you execute the **undo build** command on the management device to remove a cluster, UDP port 40000 of all the member devices in the cluster is closed at the same time.

When you execute the **undo administrator-address** command on a member device, UDP port 40000 of the member device is closed at the same time.

### Enabling NDP globally and on specific ports

**Table 573**  Enable NDP globally and on specific ports

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable NDP globally</td>
<td>ndp enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enable NDP on specified ports</td>
<td>ndp enable interface port-list</td>
<td>Required</td>
</tr>
<tr>
<td>In system view</td>
<td>interface interface-type interface-number</td>
<td>Use either approach.</td>
</tr>
</tbody>
</table>

### Enabling NTDP globally and on a specific port

**Table 574**  Enable NTDP globally and a specific port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable NTDP globally</td>
<td>ntdp enable</td>
<td>Required</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable NTDP on the port</td>
<td>ntdp enable</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Enabling the cluster function

**Table 575**  Enable the cluster function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
Cluster Configuration Tasks

Accessing the shared FTP/TFTP server from a member device

Perform the following operations in user view on a member device.

<table>
<thead>
<tr>
<th>Table 576</th>
<th>Access the shared FTP/TFTP server from a member device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Access the shared FTP server of the cluster</td>
<td><code>ftp cluster</code></td>
</tr>
<tr>
<td>Download a file from the shared TFTP server of the cluster</td>
<td><code>tftp cluster get source-file [destination-file]</code></td>
</tr>
<tr>
<td>Upload a file to the shared TFTP server of the cluster</td>
<td><code>tftp cluster put source-file [destination-file]</code></td>
</tr>
</tbody>
</table>

Managing a Cluster through the Management Device

You can manage the member devices through the management device, for example, adding/removing a cluster member, rebooting a member device, logging into a member device, and so on.

<table>
<thead>
<tr>
<th>Table 577</th>
<th>Manage a cluster through management device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enter cluster view</td>
<td><code>cluster</code></td>
</tr>
<tr>
<td>Add a candidate device to the cluster</td>
<td><code>add-member {member-number} mac-address H-H-H [password password]</code></td>
</tr>
<tr>
<td>Remove a member device from the cluster</td>
<td><code>delete-member member-number</code></td>
</tr>
<tr>
<td>Reboot a specified member device</td>
<td><code>reboot member {member-number} mac-address H-H-H [eraseflash]</code></td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>Return to user view</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>Switch between management device and member device</td>
<td>`cluster switch-to {member-number} mac-address H-H-H</td>
</tr>
<tr>
<td>Configure the MAC address of the management device</td>
<td><code>administrator-address mac-address name name</code></td>
</tr>
<tr>
<td>Configure the MAC address of the management device</td>
<td><code>mac-address mac-address vlan vlan-id [by-ip ip-address] [nondp]</code></td>
</tr>
<tr>
<td>Trace a device through MAC address or IP address</td>
<td><code>tracemac (by-mac mac-address) [by-ip ip-address] [nondp]</code></td>
</tr>
</tbody>
</table>
Enhanced cluster feature overview

1. Cluster topology management function

After the cluster topology becomes stable, you can use the topology management commands on the cluster administrative device to save the topology of the current cluster as the standard topology and back up the standard topology on the Flash memory of the administrative device.

When errors occur to the cluster topology, you can replace the current topology with the standard cluster topology and restore the administrative device using the backup topology on the Flash memory, so that the devices in the cluster can resume normal operation.

With the `display cluster current-topology` command, the switch can display the topology of the current cluster in a tree structure. The output formats include:

- Display the tree structure three layers above or below the specified node.
- Display the topology between two connected nodes.

The topology information is saved as `topology.top` in the Flash memory to the administrative device. You cannot specify the file name manually.

2. Cluster device blacklist function

To ensure stability and security of the cluster, you can use the blacklist to restrict the devices to be added to the cluster. After you add the MAC address of the device that you need to restrict into the cluster blacklist, even if the cluster function is enabled on this device and the device is normally connected to the current cluster, this device cannot join the cluster and participate in the unified management and configuration of the cluster.

Configuring the enhanced cluster features

Table 578 The enhanced cluster feature configuration tasks

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure cluster topology</td>
<td>Required</td>
<td>“Configuring cluster topology management”</td>
</tr>
<tr>
<td>management function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the cluster device</td>
<td>Required</td>
<td>“Configuring a cluster device blacklist”</td>
</tr>
<tr>
<td>blacklist</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring cluster topology management

1. Configuration prerequisites

Before configuring the cluster topology management function, make sure that:

- The basic cluster configuration is completed.
- Devices in the cluster work normally.

2. Configuration procedure
Perform the configuration instructions in Table 579 on the management device.

**Table 579  Configure cluster topology management function**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter cluster view</td>
<td>cluster</td>
<td>-</td>
</tr>
<tr>
<td>Check the current topology and save it as the standard topology.</td>
<td>topology accept { all [ save-to local-flash</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>mac-address mac-address</td>
<td>member-id member-id</td>
</tr>
<tr>
<td>Save the standard topology to the Flash memory of the administrative device</td>
<td>topology save-to local-flash</td>
<td>Required</td>
</tr>
<tr>
<td>Restore the standard topology from the Flash memory of the administrative device</td>
<td>topology restore-from local-flash</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the detailed information about a single device</td>
<td>display ntdp single-device mac-address mac-address</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the topology of the current cluster</td>
<td>display cluster current-topology [ mac-address mac-address1 [ to-mac-address mac-address2 ]</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>member-id member-id1 [ to-member-id member-id2 ] ]</td>
</tr>
<tr>
<td>Display the information about the base topology of the cluster</td>
<td>display cluster base-topology [ mac-address mac-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>member member-id ]</td>
</tr>
</tbody>
</table>

*If the management device of a cluster is a slave device in an IRF fabric, the standard topology information is saved only to the local Flash of the master device in the IRF fabric.*

**Configuring a cluster device blacklist**

Perform the configuration in Table 580 on the management device to configure a cluster device blacklist.

**Table 580  Configure the cluster device blacklist**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter cluster view</td>
<td>cluster</td>
<td>-</td>
</tr>
<tr>
<td>Add the MAC address of a specified device to the cluster blacklist</td>
<td>black-list add-mac mac-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the cluster blacklist is empty.</td>
</tr>
<tr>
<td>Displays the information about the devices in the cluster blacklist</td>
<td>display cluster black-list</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command can be executed in any view.</td>
</tr>
</tbody>
</table>
Displaying and Maintaining Cluster Configuration

After completing the above configuration, you can execute the `display` commands in any view to display the configuration and running status of cluster, so as to verify your configuration.

<table>
<thead>
<tr>
<th>Operation Description</th>
<th>Command Syntax</th>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display all NDP configuration and running information (including the interval to send NDP packets, the holdtime, and all neighbors discovered)</td>
<td><code>display ndp</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td>Display NDP configuration and running information on specified ports (including the neighbors discovered by NDP on the ports)</td>
<td><code>display ndp interface port-list</code></td>
<td></td>
</tr>
<tr>
<td>Display global NTDP information</td>
<td><code>display ntdp</code></td>
<td></td>
</tr>
<tr>
<td>Display device information collected by NTDP</td>
<td><code>display ntdp device-list [ verbose ]</code></td>
<td></td>
</tr>
<tr>
<td>Display status and statistics information about the cluster</td>
<td><code>display cluster</code></td>
<td></td>
</tr>
<tr>
<td>Display information about the candidate devices of the cluster</td>
<td>`display cluster candidates [ mac-address H-H-H</td>
<td>verbose ]`</td>
</tr>
<tr>
<td>Display information about the member devices of the cluster</td>
<td>`display cluster members [ member-number</td>
<td>verbose ]`</td>
</tr>
<tr>
<td>Clear the statistics on NDP ports</td>
<td><code>reset ndp statistics [ interface port-list ]</code></td>
<td>You can execute the <code>reset</code> command in user view.</td>
</tr>
</tbody>
</table>

When you display the cluster topology information, the devices attached to the switch that is listed in the backlist will not be displayed.

Cluster Configuration Examples

Basic Cluster Configuration Example

Network requirements

Three switches compose a cluster, where:

- The Switch 5500 serves as the management device.
- The rest are member devices.

Serving as the management device, the Switch 5500 manages the two member devices. The configuration for the cluster is as follows:

- The two member devices connect to the management device through Ethernet 1/0/2 and Ethernet 1/0/3.
- The management device connects to the Internet through Ethernet 1/0/1.
- Ethernet 1/0/1 belongs to VLAN 2, whose interface IP address is 163.172.55.1.
- All the devices in the cluster share the same FTP server and TFTP server.
The FTP server and TFTP server use the same IP address: 63.172.55.1.
The NMS and logging host use the same IP address: 69.172.55.4.

**Network diagram**

**Figure 225** Network diagram for Switch Clustering cluster configuration

---

**Configuration procedure**

1. **Configure the member devices (taking one member as an example)**

   - # Enable NDP globally and on Ethernet1/1.

   ```
   <5500> system-view
   [5500] ndp enable
   [5500] interface Ethernet 1/1
   [5500-Ethernet1/1] ndp enable
   [5500-Ethernet1/1] quit
   ```

   - # Enable NTDP globally and on Ethernet 1/1.

   ```
   [5500] ntdp enable
   [5500] interface Ethernet 1/1
   [5500-Ethernet1/1] ntdp enable
   [5500-Ethernet1/1] quit
   ```

   - # Enable the cluster function.

   ```
   [5500] cluster enable
   ```

2. **Configure the management device**

   - # Add port Ethernet 1/0/1 to VLAN 2.
<5500> system-view
[5500] vlan 2
[5500-vlan2] port Ethernet 1/0/1
[5500-vlan2] quit

# Configure the IP address of VLAN-interface 2 as 163.172.55.1.
[5500] interface Vlan-interface 2
[5500-Vlan-interface2] ip address 163.172.55.1 255.255.255.0
[5500-Vlan-interface2] quit

# Disable NDP on the uplink port Ethernet 1/0/1.
[5500] ndp enable
[5500] undo ndp enable interface Ethernet 1/0/1
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] undo ntdp enable
[5500-Ethernet1/0/1] quit

# Enable NDP on Ethernet 1/0/2 and Ethernet 1/0/3.
<5500> system-view
[5500] ndp enable
[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] ndp enable
[5500-Ethernet1/0/2] quit
[5500] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] ndp enable
[5500-Ethernet1/0/3] quit

# Set the hold time of NDP information to 200 seconds.
[5500] ndp timer aging 200

# Set the interval between sending NDP packets to 70 seconds.
[5500] ndp timer hello 70

# Enable NTDP globally and on Ethernet 1/0/2 and Ethernet 1/0/3.
[5500] ntdp enable
[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] ntdp enable
[5500-Ethernet1/0/2] quit
[5500] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] ntdp enable
[5500-Ethernet1/0/3] quit

# Set the topology collection range to 2 hops.
[5500] ntdp hop 2

# Set the delay for a member device forward topology collection requests to 150 ms.
[5500] ntdp timer hop-delay 150

# Set the delay for a member port forward topology collection requests to 15 ms.
[5500] ntdp timer port-delay 15

# Set the interval between collecting topology information to 3 minutes.
[5500] ntdp timer 3

# Enable the cluster function.
[5500] cluster enable
Cluster Configuration Examples

# Enter cluster view.
[5500] cluster
[5500-cluster]

# Configure a private IP address pool for the cluster. The IP address pool contains six IP addresses, starting from 172.16.0.1.
[5500-cluster] ip-pool 172.16.0.1 255.255.255.248

# Name and build the cluster.
[5500-cluster] build aaa
[aaa_0.3Com-cluster]

# Add the attached two switches to the cluster.
[aaa_0.3Com-cluster] add-member 1 mac-address 000f-e201-0011
[aaa_0.3Com-cluster] add-member 17 mac-address 000f-e201-0012

# Set the hold time of member device information to 100 seconds.
[aaa_0.3Com-cluster] holdtime 100

# Set the interval between sending handshake packets to 10 seconds.
[aaa_0.3Com-cluster] timer 10

# Configure VLAN-interface 2 as the network management interface.
[aaa_0.3Com-cluster] nm-interface Vlan-interface 2

# Configure the shared FTP server, TFTP server, logging host and SNMP host for the cluster.
[aaa_0.3Com-cluster] ftp-server 63.172.55.1
[aaa_0.3Com-cluster] tftp-server 63.172.55.1
[aaa_0.3Com-cluster] logging-host 69.172.55.4
[aaa_0.3Com-cluster] snmp-host 69.172.55.4

3 Perform the following operations on the member devices (taking one member as an example)

After adding the devices attached to the management device to the cluster, perform the following operations on a member device.

# Connect the member device to the remote shared FTP server of the cluster.
<aaa_1.3Com> ftp cluster

# Download the file named aaa.txt from the shared TFTP server of the cluster to the member device.
<aaa_1.3Com> tftp cluster get aaa.txt

# Upload the file named bbb.txt from the member device to the shared TFTP server of the cluster.
<aaa_1.3Com> tftp cluster put bbb.txt

- After completing the above configuration, you can execute the `cluster switch-to { member-number | mac-address H-H-H }` command on the management device to switch to member device view to maintain and manage a member device. After that, you can execute the `cluster switch-to administrator` command to return to management device view.
In addition, you can execute the `reboot member { member-number | mac-address H-H-H } [ eraseflash ]` command on the management device to reboot a member device. For detailed information about these operations, refer to the preceding description in this chapter.

After completing the above configuration, you can receive logs and SNMP trap messages of all cluster members on the NMS.

### Network Management Interface Configuration Example

#### Network requirements
- Configure VLAN-interface 2 as the network management interface of the switch;
- Configure VLAN 3 as the management VLAN;
- The IP address of the FTP server is 192.168.4.3;
- Switch A operates as the management switch;
- Switches B and C are member switches.

#### Table 582  Connection information of the management switch

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP address</th>
<th>Connection port</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 3 (connected to Switch B)</td>
<td>192.168.5.30/24</td>
<td>Ethernet 1/0/1</td>
</tr>
<tr>
<td>VLAN 2 (connect to the FTP server)</td>
<td>192.168.4.22/24</td>
<td>Ethernet 1/0/2</td>
</tr>
</tbody>
</table>

#### Network diagram

**Figure 226**  Network diagram for network management interface configuration

**Configuration procedure**

# Enter system view and configure VLAN 3 as the management VLAN.

```
<5500> system-view
[5500] management-vlan 3
```

# Add Ethernet 1/0/1 to VLAN 3.

```
[5500] vlan 3
[5500-vlan3] port Ethernet 1/0/1
[5500-vlan3] quit
```

# Set the IP address of VLAN-interface 3 to 192.168.5.30.
Cluster Configuration Examples

Enhanced Cluster Feature Configuration Example

Network requirements
- The cluster operates properly.
- Add the device with the MAC address 0001-2034-a0e5 to the cluster blacklist, that is, prevent the device from being managed and maintained by the cluster.
- Save the current cluster topology as the base topology and save it in the flash of the local management device in the cluster.
Network diagram

Figure 227  Network diagram for the enhanced cluster feature configuration

Configuration procedure

# Enter cluster view.

<aaa_0.3Com> system-view
[aaa_0.3Com] cluster

# Add the MAC address 0001-2034-a0e5 to the cluster blacklist.

[aaa_0.3Com-cluster] black-list add-mac 0001-2034-a0e5

# Backup the current topology.

[aaa_0.3Com-cluster] topology accept all save-to local-flash
PoE Configuration

PoE Overview

Introduction to PoE

Power over Ethernet (PoE)-enabled devices use twisted pairs through electrical ports to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

Advantages of PoE

- Reliability: The centralized power supply provides backup convenience, unified management, and safety.
- Easy connection: Network terminals only require an Ethernet cable, but no external power supply.
- Standard: PoE conforms to the 802.3af standard and uses a globally uniform power interfaces;
- Bright application prospect: PoE can be applied to IP phones, wireless access points (APs), chargers for portable devices, card readers, network cameras, and data collection system.

PoE components

PoE consists of three components: power sourcing equipment (PSE), PD, and power interface (PI).

- PSE: PSE is comprised of the power and the PSE functional module. It can implement PD detection, PD power information collection, PoE, power supply monitoring, and power-off for devices.
- PD: PDs receive power from the PSE. PDs include standard PDs and nonstandard PDs. Standard PDs conform to the 802.3af standard, including IP phones, Wireless APs, network cameras and so on.
- PI: PIs are RJ45 interfaces which connect PSE/PDs to network cables.

PoE Features Supported by the Switch 5500

PoE-enabled Switch 5500s:

- Switch 5500-EI PWR 28-Port
- Switch 5500-EI PWR 52-Port
- Switch 5500G 24-Port
- Switch 5500G 48-Port

A PoE-enabled Switch 5500 has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to PDs that do not support the 802.3af standard.
It can deliver data and current simultaneously through data wires (1, 2, 3, and 6) of category-3/5 twisted pairs.

Through the fixed 24/48 Ethernet electrical ports, it can supply power to up to 24/48 remote Ethernet switches with a maximum distance of 100 m (328 feet).

Each Ethernet electrical port can supply at most a power of 15,400 mW to a PD.

When AC power input is adopted for the switch, the maximum total power that can be provided is 300 W. The switch can determine whether to supply power to the next remote PD it detects depending on its available power.

When DC power input is adopted for the switch, it is capable of supplying full power to all of the 24/48 ports, that is, 15,400 mW for each port, and the total power is 369.6 W/739.2 W.

The PSE processing software on the switch can be upgraded online.

The switch provides statistics about power supplying on each port and the whole equipment, which you can query through the `display` command.

The switch provides two modes (auto and manual) to manage the power feeding to ports in the case of PSE power overload.

The switch provides over-temperature protection mechanism. Using this mechanism, the switch disables the PoE feature on all ports when its internal temperature exceeds 65°C (149°F) for self-protection, and restores the PoE feature on all its ports when the temperature drops below 60°C (140°F).

The switch supports the PoE profile feature, that is, different PoE policies can be set for different user groups. These PoE policies are each saved in the corresponding PoE profile and applied to ports of the user groups.

When you use the PoE-enabled Switch 5500 to supply power, the PDs need no external power supply.

If a remote PD has an external power supply, the PoE-enabled Switch 5500 and the external power supply will backup each other for the PD.

Only the 100 Mbps Ethernet electrical ports of the PoE-enabled Switch 5500 support the PoE feature.

---

### PoE Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Enabling the PoE Feature on a Port”</td>
<td>Required</td>
</tr>
<tr>
<td>“Setting the Maximum Output Power on a Port”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting PoE Management Mode and PoE Priority of a Port”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting the PoE Mode on a Port”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the PD Compatibility Detection Function”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring PoE Over-Temperature Protection on the Switch”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Upgrading the PSE Processing Software Online”</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Enabling the PoE Feature on a Port

**CAUTION:**
- By default, the PoE function on a port is enabled by the default configuration file (config.def) when the device is delivered.
- If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device.

Setting the Maximum Output Power on a Port

The maximum power that can be supplied by each Ethernet electrical port of a PoE-enabled Switch 5500 to its PD is 15,400 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, in the range of 1,000 to 15,400 mW and in the granularity of 100 mW.

Setting PoE Management Mode and PoE Priority of a Port

When a switch is close to its full load in supplying power, you can adjust the power supply of the switch through the cooperation of the PoE management mode and the port PoE priority settings. The Switch 5500 supports two PoE management modes, auto and manual. The auto mode is adopted by default.

- **auto:** When the switch is close to its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and then supply power to the PDs that are connected to the ports with high priority. For example: Port A has the priority of critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch will power down the PD connected to the port with the lowest priority and turn to supply power to this new PD. If more than one port has the same lowest priority, the switch will power down the PD connected to the port with larger port number.

---

### Table 583  PoE configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Upgrading the PSE Processing Software of Fabric Switches Online”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Displaying PoE Configuration”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### Table 584  Enable the PoE feature on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable the PoE feature on a port</td>
<td>poe enable</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Table 585  Set the maximum output power on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Set the maximum output power on the port</td>
<td>poe max-power max-power</td>
<td>Required 15,400 mW by default.</td>
</tr>
</tbody>
</table>
- **manual**: When the switch is close to its full load in supplying power, it will not make change to its original power supply status based on its priority when a new PD is added. For example: Port A has the priority critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch just gives a prompt that a new PD is added and will not supply power to this new PD.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE management mode and PoE priority of a port.

### Table 586  Set a port’s PoE management mode and PoE priority

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Set the PoE management mode for the switch</td>
<td>`poe power-management { auto</td>
<td>manual }`</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Set the PoE priority of a port</td>
<td>`poe priority { critical</td>
<td>high</td>
</tr>
</tbody>
</table>

**Setting the PoE Mode on a Port**

PoE mode of a port falls into two types, signal mode and spare mode.

- **Signal mode**: DC power is carried over the data pairs (1,2,3, and 6) of category-3/5 twisted pairs.
- **Spare mode**: DC power is carried over the spare pairs (4,5,7, and 8) of category-3/5 twisted pairs.

Currently, the Switch 5500 does not support the spare mode.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE mode on a port.

### Table 587  Set the PoE mode on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Set the PoE mode on the port to signal</td>
<td><code>poe mode signal</code></td>
<td>Optional signal by default.</td>
</tr>
</tbody>
</table>

**Configuring the PD Compatibility Detection Function**

After the PD compatibility detection function is enabled, the switch can detect the PDs that do not conform to the 802.3af standard and supply power to them.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection function.
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

### Table 588 Configure the PD compatibility detection function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the PD compatibility</td>
<td>poe legacy enable</td>
<td>Required</td>
</tr>
<tr>
<td>detection function</td>
<td></td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>

Caution: If you adjust the PD disconnection detection mode when the switch is running, the connected PDs will be powered off. Therefore, be cautious to do so.

Configuring PoE Over-Temperature Protection on the Switch

If this function is enabled, the switch disables the PoE feature on all ports when its internal temperature exceeds 65°C (149°F) for self-protection, and restores the PoE feature settings on all its ports when the temperature drops below 60°C (140°F).

### Table 590 Configure PoE over-temperature protection on the switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable PoE over-temperature protection on the</td>
<td>poe temperature-protection enable</td>
<td>Optional</td>
</tr>
<tr>
<td>switch</td>
<td></td>
<td>Enabled by default.</td>
</tr>
</tbody>
</table>

- When the internal temperature of the switch decreases from \( X \) \( (X>65 \, ^\circ \text{C}, \text{ or } X>149 \, ^\circ \text{F}) \) to \( Y \) \( (60 \, ^\circ \text{C} \leq Y < 65 \, ^\circ \text{C}, \text{ or } 140 \, ^\circ \text{F} < Y < 149 \, ^\circ \text{F}) \), the switch still keeps the PoE function disabled on all the ports.

- When the internal temperature of the switch increases from \( X \) \( (X<60 \, ^\circ \text{C}, \text{ or } X<140 \, ^\circ \text{F}) \) to \( Y \) \( (60 \, ^\circ \text{C} < Y \leq 65 \, ^\circ \text{C}, \text{ or } 140 \, ^\circ \text{F} \leq Y < 149 \, ^\circ \text{F}) \), the switch still keeps the PoE function enabled on all the ports.

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. Before performing the following configuration, download the PSE processing software to the Flash of the switch.

### Table 591 Upgrade PSE processing software online

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
In the case that the PSE processing software is damaged (that is, no `PoE` command can be executed successfully), use the `full` update mode to upgrade and thus restore the software.

The `refresh` update mode is to upgrade the original processing software in the PSE through refreshing the software, while the `full` update mode is to delete the original processing software in PSE completely and then reload the software.

Generally, the `refresh` update mode is used to upgrade the PSE processing software.

When the online upgrading procedure is interrupted for some unexpected reason (for example, the device restarts due to some errors), if the upgrade in `full` mode fails after restart, you must upgrade in `full` mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.

### Upgrading the PSE Processing Software of Fabric Switches Online

You can update or repair the damaged PSE processing software by upgrading it. By executing the following command on any device in the fabric, you can upgrade the PSE processing software of all devices in the fabric by using the specified PSE processing software. For fabric details, see “IRF Fabric Configuration” on page 733.

#### Table 591  Upgrade PSE processing software online

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade the PSE processing software online</td>
<td>`poe update { refresh</td>
<td>full } filename`</td>
</tr>
</tbody>
</table>

### Displaying PoE Configuration

After completing the above configuration, execute the `display` command in any view to see the operation of the PoE feature and verify the effect of the configuration.
PoE Configuration Example

Network requirements
Switch A is a Switch 5500 that supports PoE, Switch B can be PoE powered.

- The Ethernet 1/0/1 and Ethernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the Ethernet 1/0/8 port is intended to be connected with an important AP.
- The PSE processing software of Switch A is first upgraded online. The remotely accessed PDs are powered by Switch A.
- The power consumption of the accessed AP is 2,500 mW, and the maximum power consumption of Switch B is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the Ethernet 1/0/8 port even when Switch A is under full load.

Networking diagram

Table 593  Display PoE configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current PD disconnection detection mode of the switch</td>
<td>display poe disconnect</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the PoE status of a specific port or all ports of the switch</td>
<td>display poe interface</td>
<td></td>
</tr>
<tr>
<td>Display the PoE power information of a specific port or all ports of the switch</td>
<td>display poe interface power</td>
<td></td>
</tr>
<tr>
<td>Display the PSE parameters</td>
<td>display poe powersupply</td>
<td></td>
</tr>
<tr>
<td>Display the status (enabled/disabled) of the PoE over-temperature protection feature on the switch</td>
<td>display poe temperature-protection</td>
<td></td>
</tr>
</tbody>
</table>
Configuration procedure

# Upgrade the PSE processing software online.

<SwitchA> system-view
[SwitchA] poe update refresh 0290_021.s19

# Enable the PoE feature on Ethernet 1/0/1, and set the PoE maximum output power of Ethernet 1/0/1 to 12,000 mW.

[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] poe enable
[SwitchA-Ethernet1/0/1] poe max-power 12000
[SwitchA-Ethernet1/0/1] quit

# Enable the PoE feature on Ethernet 1/0/2, and set the PoE maximum output power of Ethernet 1/0/2 to 2500 mW.

[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] poe enable
[SwitchA-Ethernet1/0/2] poe max-power 2500
[SwitchA-Ethernet1/0/2] quit

# Enable the PoE feature on Ethernet 1/0/8, and set the PoE priority of Ethernet 1/0/8 to critical.

[SwitchA] interface Ethernet 1/0/8
[SwitchA-Ethernet1/0/8] poe enable
[SwitchA-Ethernet1/0/8] poe priority critical
[SwitchA-Ethernet1/0/8] quit

# Set the PoE management mode on the switch to auto (it is the default mode, so this step can be omitted).

[SwitchA] poe power-management auto

# Enable the PD compatibility detect of the switch to allow the switch to supply power to part of the devices noncompliant with the 802.3af standard.

[SwitchA] poe legacy enable
**Introduction to PoE Profile**

On a large-sized network or a network with mobile users, to help network administrators monitor the switch's PoE features, the Switch 5500 provides the PoE profile features. A PoE profile is a set of PoE configurations, including multiple PoE features.

Features of PoE profile:

- Various PoE profiles can be created. PoE policy configurations applicable to different user groups are stored in the corresponding PoE profiles. These PoE profiles can be applied to the ports used by the corresponding user groups.
- When users connect a PD to a PoE-profile-enabled port, the PoE configurations in the PoE profile will be enabled on the port.

---

**PoE Profile Configuration**

**Configuring PoE Profile**

<table>
<thead>
<tr>
<th>Table 594</th>
<th>Configure PoE profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Create a PoE profile and enter PoE profile view</td>
<td>poe-profile profilename</td>
</tr>
<tr>
<td>If the PoE file is created, you will enter PoE profile view directly through the command.</td>
<td></td>
</tr>
<tr>
<td>Configure the relevant features in PoE profile</td>
<td>poe enable</td>
</tr>
<tr>
<td>Enable the PoE feature on a port</td>
<td>poe mode signal</td>
</tr>
<tr>
<td>Configure PoE mode for Ethernet ports</td>
<td>spare</td>
</tr>
<tr>
<td>Signal by default.</td>
<td></td>
</tr>
<tr>
<td>Configure the PoE priority for Ethernet ports</td>
<td>poe priority critical</td>
</tr>
<tr>
<td>high</td>
<td>low</td>
</tr>
<tr>
<td>Configure the maximum power for Ethernet ports</td>
<td>poe max-power</td>
</tr>
<tr>
<td>max-power</td>
<td>15,400 mW by default.</td>
</tr>
<tr>
<td>Quit system view</td>
<td>quit</td>
</tr>
</tbody>
</table>
Note the following during the configuration:

1. When the `apply poe-profile` command is used to apply a PoE profile to a port, some PoE features in the PoE profile can be applied successfully while some cannot. PoE profiles are applied to the Switch 5500 according to the following rules:

   - When the `apply poe-profile` command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the `display current-configuration` command is used for query, it is displayed that the PoE profile is applied properly to the port.
   - If one or more features in the PoE profile are not applied properly on a port, the switch will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
   - The `display current-configuration` command can be used to query which PoE profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.

2. PoE profile configuration is a global configuration, and applies synchronously in the Intelligent Resilient Framework (IRF) system.

3. Combination of Unit creates a new Fabric. In the newly created Fabric, the PoE profile configuration of the Unit with the smallest Unit ID number will become the PoE profile configuration for the Fabric currently in use.

4. Split of Fabric results in many new Fabrics. In each newly created Fabric, the PoE profile configuration of each Unit remains the same as it was before the split.

### Displaying PoE Profile Configuration

After completing the above configuration, execute the `display` command in any view to see the running status of the PoE profile and verify the effect of the configuration by checking the displayed information.

#### Table 594 Configure PoE profile

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the existing PoE profile to the specified Ethernet port in system view</td>
<td><code>apply poe-profile profile-name interface interface-type interface-number [ to interface-type interface-number ]</code></td>
<td>Use either approach.</td>
</tr>
<tr>
<td>In Ethernet port view</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Apply the existing PoE profile to the port</td>
<td><code>apply poe-profile profile-name</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 595 Display the PoE profile configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the detailed information about the PoE profiles created on the switch</td>
<td>`display poe-profile { all-profile</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
PoE Profile Configuration Example

PoE Profile Application Example

Network requirements
Switch A is a Switch 5500 that supports PoE.

- Ethernet 1/0/1 through Ethernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:
  - The PoE function can be enabled on all ports in use.
  - Signal mode is used to supply power.
  - The PoE priority for Ethernet 1/0/1 through Ethernet 1/0/5 is Critical, whereas the PoE priority for Ethernet 1/0/6 through Ethernet 1/0/10 is High.
  - The maximum power for Ethernet 1/0/1 through Ethernet 1/0/5 ports is 3,000 mW, whereas the maximum power for Ethernet 1/0/6 through Ethernet 1/0/10 is 15,400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet 1/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet 1/0/6 through Ethernet 1/0/10.

Network diagram

Figure 229 PoE profile application
Configuration procedure

# Create Profile 1, and enter PoE profile view.

<SwitchA> system-view
[SwitchA] poe-profile Profile1

# In Profile 1, add the PoE policy configuration applicable to Ethernet 1/0/1 through Ethernet 1/0/5 ports for users of group A.

[SwitchA-poe-profile-Profile1] poe enable
[SwitchA-poe-profile-Profile1] poe mode signal
[SwitchA-poe-profile-Profile1] poe priority critical
[SwitchA-poe-profile-Profile1] poe max-power 3000
[SwitchA-poe-profile-Profile1] quit

# Display detailed configuration information for Profile1.

[SwitchA] display poe-profile name Profile1
Poe-profile: Profile1, 3 action
    poe enable
    poe max-power 3000
    poe priority critical

# Create Profile 2, and enter PoE profile view.

[SwitchA] poe-profile Profile2

# In Profile 2, add the PoE policy configuration applicable to Ethernet 1/0/6 through Ethernet 1/0/10 ports for users of group A.

[SwitchA-poe-profile-Profile2] poe enable
[SwitchA-poe-profile-Profile2] poe mode signal
[SwitchA-poe-profile-Profile2] poe priority high
[SwitchA-poe-profile-Profile2] poe max-power 15400
[SwitchA-poe-profile-Profile2] quit

# Display detailed configuration information for Profile2.

[SwitchA] display poe-profile name Profile2
Poe-profile: Profile2, 2 action
    poe enable
    poe priority high

# Apply the configured Profile 1 to Ethernet 1/0/1 through Ethernet 1/0/5 ports.

[SwitchA] apply poe-profile Profile1 interface Ethernet1/0/1 to Ethernet1/0/5

# Apply the configured Profile 2 to Ethernet 1/0/6 through Ethernet 1/0/10 ports.

[SwitchA] apply poe-profile Profile2 interface Ethernet1/0/6 to Ethernet1/0/10
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 Switch 5500 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.
- Otherwise, the device sends the packet to the upper layer protocol for processing.

Relay forwarding of BOOTP/DHCP broadcast packets is implemented by the DHCP relay function using UDP ports 67 and 68, so these two ports cannot be configured as UDP Helper relay ports.

By default, with UDP Helper enabled, the device forwards broadcast packets with the six UDP destination port numbers listed in Table 596.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>UDP port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS (Domain Name System)</td>
<td>53</td>
</tr>
<tr>
<td>NetBIOS-DS (NetBIOS Datagram Service)</td>
<td>138</td>
</tr>
<tr>
<td>NetBIOS-NS (NetBIOS Name Service)</td>
<td>137</td>
</tr>
<tr>
<td>TACACS (Terminal Access Controller Access Control System)</td>
<td>49</td>
</tr>
<tr>
<td>TFTP (Trivial File Transfer Protocol)</td>
<td>69</td>
</tr>
<tr>
<td>Time Service</td>
<td>37</td>
</tr>
</tbody>
</table>
Configuring UDP Helper

On the Switch 5500, the reception of directed broadcast packets to a directly connected network is disabled by default. As a result, UDP Helper is available only when the `ip forward-broadcast` command is configured in system view. For details about the `ip forward-broadcast` command, refer to “IP Addressing Configuration” on page 123 and “IP Performance Configuration” on page 129.

You need to enable UDP Helper before specifying any UDP port to match UDP broadcasts; otherwise, the configuration fails. When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.

The `dns`, `netbios-ds`, `netbios-ns`, `tacacs`, `tftp`, and `time` keywords correspond to the six default ports. You can configure the default ports by specifying port numbers or the corresponding parameters. For example, `udp-helper port 53` and `udp-helper port dns` specify the same port.

You can specify up to 20 destination server addresses on a VLAN interface.

If UDP Helper is enabled after a destination server is configured for a VLAN interface, the broadcasts from interfaces belonging to the VLAN and having a matching UDP port will be unicast to the destination server.

Displaying and Maintaining UDP Helper

After performing the above configurations, use the `display` command in any view to display the running status of the UDP Helper configuration, and verify the configuration result. Use the `reset` command in user view to clear statistics about packets forwarded by UDP Helper.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable UDP Helper</td>
<td><code>udp-helper enable</code></td>
<td>Required Disabled by default.</td>
</tr>
<tr>
<td>Enable the device to receive directed broadcasts</td>
<td><code>ip forward-broadcast</code></td>
<td>Required By default, the device is disabled from receiving directed broadcasts.</td>
</tr>
<tr>
<td>Enable UDP Helper</td>
<td><code>udp-helper enable</code></td>
<td>Required Disabled by default.</td>
</tr>
<tr>
<td>Specify a UDP port number</td>
<td>`udp-helper port {port-number</td>
<td>dns</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface vlan-interface vlan-id</code></td>
<td>-</td>
</tr>
<tr>
<td>Specify the destination server to which the UDP packets are to be forwarded</td>
<td><code>udp-helper server ip-address</code></td>
<td>Required No destination server is specified by default.</td>
</tr>
</tbody>
</table>
Cross-Network Computer Search Through UDP Helper

Network requirements
PC A resides on network segment 192.168.1.0/24 and PC B on 192.168.10.0/24; they are connected through Switch A and are routable to each other. It is required to configure UDP Helper on the switch, so that PC A can find PC B through computer search. (Broadcasts with UDP port 137 are used for searching.)

Network diagram

Figure 230 Network diagram for UDP Helper configuration

Configuration procedure
# Enable Switch A to receive directed broadcasts to a directly connected network.

<5500> system-view
[5500] ip forward-broadcast

# Enable UDP Helper on Switch A.

[5500] udp-helper enable

# Configure the switch to forward broadcasts containing the destination UDP port number 137. (By default, the device enabled with UDP Helper forwards the broadcasts containing the destination UDP port number 137.)

[5500] udp-helper port 137

# Specify the destination server IP address on Vlan-interface 1.

[5500] interface Vlan-interface 1
[5500-Vlan-interface1] udp-helper server 192.168.10.2

Table 230 Display and maintain UDP Helper configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the UDP broadcast relay forwarding information of a specified VLAN interface on the switch</td>
<td>display udp-helper server interface vlan-interface vlan-id</td>
<td>You can use the display command in any view</td>
</tr>
<tr>
<td>Clear statistics about packets forwarded by UDP Helper</td>
<td>reset udp-helper packet</td>
<td>You can use the reset command in user view</td>
</tr>
</tbody>
</table>
**SNMP Overview**

The Simple Network Management Protocol (SNMP) is used for ensuring the transmission of the management information between any two network nodes. In this way, network administrators can easily retrieve and modify the information about any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

As SNMP adopts the polling mechanism and provides basic function set, it is suitable for small-sized networks with fast-speed and low-cost. SNMP is based on User Datagram Protocol (UDP) and is thus widely supported by many products.

---

**SNMP Operation Mechanism**

SNMP is implemented by two components, namely, Network Management Station (NMS) and agent.

- An NMS can be a workstation running client program. At present, the commonly used network management platforms include Sun NetManager and IBM NetView.
- Agent is server-side software running on network devices (such as switches).

An NMS can send GetRequest, GetNextRequest and SetRequest messages to the agents. Upon receiving the requests from the NMS, an agent performs Read or Write operation on the managed object (MIB, Management Information Base) according to the message types, generates the corresponding Response packets and returns them to the NMS.

When a network device operates improperly or changes to other state, the agent on it can also send trap messages on its own initiative to the NMS to report the events.

---

**SNMP Versions**

Currently, SNMP agent on a switch supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c.

SNMPv3 adopts user name and password authentication.

SNMPv1 and SNMPv2c adopt community name authentication. The SNMP packets containing invalid community names are discarded. SNMP community name is used to define the relationship between SNMP NMS and SNMP agent. Community name functions as password. It can limit accesses made by SNMP NMS to SNMP agent. You can perform the following community name-related configuration.

- Specifying MIB view that a community can access.
- Set the permission for a community to access an MIB object to be read-only or read-write. Communities with read-only permissions can only query the switch...
information, while those with read-write permission can configure the switch as well.

- Set the basic ACL specified by the community name.

**Supported MIBs**

An SNMP packet carries management variables with it. Management variable is used to describe the management objects of a switch. To uniquely identify the management objects of the switch, SNMP adopts a hierarchical naming scheme to organize the managed objects. It is like a tree, with each tree node representing a managed object, as shown in Figure 231. Each node in this tree can be uniquely identified by a path starting from the root.

![Architecture of the MIB tree](image)

The management information base (MIB) describes the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network devices. In the above figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. The number string is the object identifier (OID) of the managed object.

The common MIBs supported by switches are listed in Table 599.

**Table 599** Common MIBs

<table>
<thead>
<tr>
<th>MIB attribute</th>
<th>MIB content</th>
<th>Related RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public MIB</td>
<td>MIB II based on TCP/IP network device</td>
<td>RFC 1213</td>
</tr>
<tr>
<td></td>
<td>BRIDGE MIB</td>
<td>RFC 1493</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RFC 2675</td>
</tr>
<tr>
<td>RIP MIB</td>
<td></td>
<td>RFC 1724</td>
</tr>
<tr>
<td>RMON MIB</td>
<td></td>
<td>RFC 2819</td>
</tr>
<tr>
<td>Ethernet MIB</td>
<td></td>
<td>RFC 2665</td>
</tr>
<tr>
<td>OSPF MIB</td>
<td></td>
<td>RFC 1253</td>
</tr>
<tr>
<td>IF MIB</td>
<td></td>
<td>RFC 1573</td>
</tr>
</tbody>
</table>
Configuring Basic SNMP Functions

SNMPv3 configuration is quite different from that of SNMPv1 and SNMPv2c. Therefore, the configuration of basic SNMP functions is described by SNMP versions, as listed in Table 600 and Table 601.

Switches now support configuring SNMPv3 users by using the Advanced Encryption Standard (AES), which is the new encryption standard in place of Data Encryption Standard (DES).

### Table 599  Common MIBs

<table>
<thead>
<tr>
<th>MIB attribute</th>
<th>MIB content</th>
<th>Related RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private MIB</td>
<td>DHCP MIB</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>QACL MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSTP MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPV6 ADDRESS MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MIRRORGROUP MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QINQ MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.x MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch Clustering MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NTP MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface management</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Basic SNMP Functions

Switches now support configuring SNMPv3 users by using the Advanced Encryption Standard (AES), which is the new encryption standard in place of Data Encryption Standard (DES).

### Table 600  Configure basic SNMP functions (SNMPv1 and SNMPv2c)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable SNMP agent</td>
<td>snmp-agent</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can enable SNMP agent by executing this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>command or any of the commands used to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure SNMP agent.</td>
</tr>
</tbody>
</table>

Set system information, and specify to enable SNMPv1 or SNMPv2c on the switch

```
snmp-agent sys-info {
  contact sys-contact |
  location sys-location |
  version {{ v1 | v2c | v3 }* | all }}
```

Required

By default, the contact information for system maintenance is , 3Com and the SNMP version is SNMPv3.
### Table 600  Configure basic SNMP functions (SNMPv1 and SNMPv2c)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set a community name and access permission</td>
<td>snmp-agent community { read</td>
<td>write } community-name [ acl acl-number</td>
</tr>
<tr>
<td>Indirect configuration</td>
<td>snmp-agent group { v1</td>
<td>v2c } group-name [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]</td>
</tr>
<tr>
<td>Indirect configuration</td>
<td>snmp-agent usm-user { v1</td>
<td>v2c } user-name group-name [ acl acl-number ]</td>
</tr>
<tr>
<td>Add a user to an SNMP group</td>
<td>snmp-agent packet max-size byte-count</td>
<td>Optional</td>
</tr>
<tr>
<td>Set the maximum size of an SNMP packet for SNMP agent to receive or send</td>
<td>snmp-agent local-switch fabricid switch fabricid</td>
<td>Optional</td>
</tr>
<tr>
<td>Set the device switch fabric ID</td>
<td>snmp-agent mib-view { included</td>
<td>excluded } view-name oid-tree [ mask mask-value ]</td>
</tr>
<tr>
<td>Create/Update the view information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 601  Configure basic SNMP functions (SNMPv3)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable SNMP agent</td>
<td>snmp-agent</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.</td>
</tr>
<tr>
<td>Set system information and specify to enable SNMPv3 on the switch</td>
<td>snmp-agent sys-info { contact sys-contact</td>
<td>location sys-location</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the contact information for system maintenance is 3Com and the SNMP version is SNMPv3.</td>
</tr>
<tr>
<td>Set an SNMP group</td>
<td>snmp-agent group v3 group-name [ authentication</td>
<td>privacy ] [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]</td>
</tr>
</tbody>
</table>
Configuring Trap-Related Functions

Configuring Basic Trap Functions

Table 601 Configure basic SNMP functions (SNMPv3)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt a plain-text password to generate a cipher-text one</td>
<td>`snmp-agent calculate-password plain-password mode { md5</td>
<td>sha } ( local-switch fabricid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command is used if password in cipher-text is needed for adding a new user.</td>
</tr>
<tr>
<td>Add a user to an SNMP group</td>
<td>`snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5</td>
<td>sha } auth-password [ privacy-mode { des56</td>
</tr>
<tr>
<td>Set the maximum size of an SNMP packet for SNMP agent to receive or send</td>
<td><code>snmp-agent packet max-size byte-count</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1,500 bytes by default.</td>
</tr>
<tr>
<td>Set the device switch fabric ID</td>
<td><code>snmp-agent local-switch fabricid switch fabricid</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the device switch fabric ID is <code>enterprise number + device information</code>.</td>
</tr>
<tr>
<td>Create or update the view information</td>
<td>`snmp-agent mib-view { included</td>
<td>excluded } view-name oid-tree [ mask mask-value ]`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the view name is <code>ViewDefault</code> and OID is 1.</td>
</tr>
</tbody>
</table>

A Switch 5500 provides the following functions to prevent attacks through unused UDP ports.

- Executing the `snmp-agent` command or any of the commands used to configure the SNMP agent enables the SNMP agent, and at the same time opens UDP port 161 used by SNMP agents and the UDP port used by the SNMP trap respectively.
- Executing the `undo snmp-agent` command disables the SNMP agent and closes the UDP ports used by the SNMP agent and SNMP trap.
CHAPTER 68: SNMP CONFIGURATION

Configuring the Extended Trap Function

The extended Trap function refers to adding an interface description and interface type into the linkUp/linkDown Trap message. When receiving this extended Trap message, NMS can immediately determine which interface on the device fails according to its interface description and type.

Table 603  Configuring the extended Trap function

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the extended Trap function</td>
<td>snmp-agent trap ifmib link extended</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the linkUp/linkDown Trap message adopts the standard format defined in IF-MIB. For details, refer to RFC 1213.</td>
</tr>
</tbody>
</table>
Enabling Logging for Network Management

When SNMP logging is enabled on a device, SNMP logs are output to the device’s information center. With the output destinations of the information center set, the output destinations of the SNMP logs are decided.

The severity level of the SNMP logs is informational, that is, the logs are taken as general prompt information of the device. To view the SNMP logs, enable the information center to output system information with the informational level.

For a detailed description of the system information and information center, refer to “Information Center” on page 899.

Displaying SNMP

After completing the above configuration, you can execute the display command in any view to view the running status of SNMP, and to verify the configuration.

<table>
<thead>
<tr>
<th>Table 604 Enable logging for network management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Enable logging for network management</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 605 Display SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Display the SNMP information about the current device</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Display SNM packet statistics</td>
</tr>
<tr>
<td>Display the switch fabric ID of the current device</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Display group information about the device</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Display SNMP user information</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Display Trap list information</td>
</tr>
<tr>
<td>Display the currently configured community name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Display the currently configured MIB view</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
SNMP Configuration Example

Network requirements

- An NMS and Switch A (SNMP agent) are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.
- Perform the following configuration on Switch A: setting the community name and access permission, administrator ID, contact and switch location, and enabling the switch to sent trap messages.

Thus, the NMS is able to access Switch A and receive the trap messages sent by Switch A.

Network diagram

Figure 232 Network diagram for SNMP configuration

Network procedure

# Enable SNMP agent, and set the SNMPv1 and SNMPv2c community names.

```bash
<5500> system-view
[5500] snmp-agent
[5500] snmp-agent sys-info version all
[5500] snmp-agent community read public
[5500] snmp-agent community write private
```

# Set the access right of the NMS to the MIB of the SNMP agent.

```bash
[5500] snmp-agent mib-view include internet 1.3.6.1
```

# For SNMPv3, set:

- SNMPv3 group and user
- security to the level of needing authentication and encryption
- authentication protocol to HMAC-MD5
- authentication password to passmd5
- encryption protocol to AES
- encryption password to cfb128cfb128

```bash
[5500] snmp-agent group v3 managev3group privacy write-view internet
[5500] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5 passmd5 privacy-mode aes128 cfb128cfb128
```
# Set the VLAN-interface 2 as the interface used by NMS. Add port Ethernet 1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[5500] vlan 2
[5500-vlan2] port Ethernet 1/0/2
[5500-vlan2] quit
[5500] interface Vlan-interface 2
[5500-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[5500-Vlan-interface2] quit
```

# Enable the SNMP agent to send Trap messages to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is `public`.

```
[5500] snmp-agent trap enable standard authentication
[5500] snmp-agent trap enable standard coldstart
[5500] snmp-agent trap enable standard linkup
[5500] snmp-agent trap enable standard linkdown
[5500] snmp-agent target-host trap address udp-domain 10.10.10.1 udp -port 5000 params securityname public
```

**Configuring the NMS**

The Switch 5500 supports 3Com’s Netork Management System (NMS). SNMPv3 adopts user name and password authentication. When you use 3Com’s NMS, you need to set user names and choose the security level in [Authentication Parameter]. For each security level, you need to set authorization mode, authorization password, encryption mode, encryption password, and so on. In addition, you need to set timeout time and maximum retry times.

You can query and configure an Ethernet switch through the NMS. For more information, refer to the corresponding documentation provided by the NMS product.

> Authentication-related configuration on an NMS must be consistent with that of the devices for the NMS to manage the devices successfully.
Introduction to RMON

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF). It is an important enhancement made to MIB II standards. RMON is mainly used to monitor the data traffic across a network segment or even the entire network, and is currently a commonly used network management standard.

An RMON system comprises of two parts: the network management station (NMS) and the agents running on network devices. RMON agents operate on network monitors or network probes to collect and keep track of the statistics of the traffic across the network segments to which their ports connect, such as the total number of the packets on a network segment in a specific period of time and the total number of packets successfully sent to a specific host.

- RMON is fully based on SNMP architecture. It is compatible with the current SNMP implementations.
- RMON enables SNMP to monitor remote network devices more effectively and actively, thus providing a satisfactory means of monitoring remote subnets.
- With RMON implemented, the communication traffic between NMS and SNMP agents can be reduced, thus facilitating the management of large-scale internetworks.

Working Mechanism of RMON

RMON allows multiple monitors. It can collect data in the following two ways:

- Using the dedicated RMON probes. When an RMON system operates in this way, the NMS directly obtains management information from the RMON probes and controls the network resources. In this case, all information in the RMON MIB can be obtained.

- Embedding RMON agents into network devices (such as routers, switches and hubs) directly to make the latter capable of RMON probe functions. When an RMON system operates in this way, the NMS collects network management information by exchanging information with the SNMP agents using the basic SNMP commands. However, this way depends on device resources heavily and an NMS operating in this way can only obtain the information about these four groups (instead of all the information in the RMON MIB): alarm group, event group, history group, and statistics group.

The 3Com Switch 5500 implements RMON in the second way. With an RMON agent embedded, the Switch 5500 can serve as a network device with the RMON probe function. Through the RMON-capable SNMP agents running on the switch, an NMS can obtain the information about the total traffic, error statistics and performance statistics of the network segments to which the ports of the
managed network devices are connected. Thus, the NMS can further manage the networks.

**Commonly Used RMON Groups**

**Event group**

Event group is used to define the indexes of events and the processing methods of the events. The events defined in an event group are mainly used by entries in the alarm group and extended alarm group to trigger alarms.

You can specify a network device to act in one of the following ways in response to an event:

- Logging the event
- Sending trap messages to the NMS
- Logging the event and sending trap messages to the NMS
- No processing

**Alarm group**

RMON alarm management enables monitoring on specific alarm variables (such as the statistics of a port). When the value of a monitored variable exceeds the threshold, an alarm event is generated, which then triggers the network device to act in the way defined in the events. Events are defined in event groups.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sampling the defined alarm variables periodically
- Comparing the samples with the threshold and triggering the corresponding events if the former exceed the latter

**Extended alarm group**

With extended alarm entry, you can perform operations on the samples of alarm variables and then compare the operation results with the thresholds, thus implement more flexible alarm functions.

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions periodically
- Performing operations on the samples according to the defined expressions
- Comparing the operation results with the thresholds and triggering corresponding events if the operation result exceeds the thresholds

**History group**

After a history group is configured, the Ethernet switch collects network statistics information periodically and stores the statistics information temporarily for later use. A history group can provide the history data of the statistics on network segment traffic, error packets, broadcast packets, and bandwidth utilization.
With the history data management function, you can configure network devices to collect history data, sample and store data of a specific port periodically.

**Statistics group**

Statistics group contains the statistics of each monitored port on a switch. An entry in a statistics group is an accumulated value counting from the time when the statistics group is created.

The statistics include the number of the following items: collisions, packets with Cyclic Redundancy Check (CRC) errors, undersize (or oversize) packets, broadcast packets, multicast packets, and received bytes and packets.

With the RMON statistics management function, you can monitor the use of a port and make statistics on the errors occurred when the ports are being used.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Add an event entry</td>
<td>rmon event event-entry [description string ] {log</td>
<td>trap trap-community</td>
</tr>
<tr>
<td>Add an alarm entry</td>
<td>rmon alarm entry-number alarm-variable sampling-time {delta</td>
<td>absolute} rising_threshold threshold-value1 event-entry1 falling_threshold threshold-value2 event-entry2 [owner text ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Before adding an alarm entry, you need to use the rmon event command to define the event to be referenced by the alarm entry.</td>
</tr>
<tr>
<td>Add an extended alarm entry</td>
<td>rmon prialarm entry-number prialarm-formula prialarm-des sampling-timer {delta</td>
<td>absolute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Before adding an extended alarm entry, you need to use the rmon event command to define the event to be referenced by the extended alarm entry.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Add a history entry</td>
<td>rmon history entry-number buckets number interval sampling-interval [owner text ]</td>
<td>Optional</td>
</tr>
<tr>
<td>Add a statistics entry</td>
<td>rmon statistics entry-number [owner text ]</td>
<td>Optional</td>
</tr>
</tbody>
</table>
The `rmon alarm` and `rmon prialarm` commands take effect on existing nodes only.

For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, you will fail to create another statistics entry with a different index for the same port.

### Displaying RMON

After completing the above configuration, you can execute the `display` command in any view to display the RMON running status, and to verify the configuration.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display RMON statistics</td>
<td>`display rmon statistics [interface-type</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>unit</td>
</tr>
<tr>
<td>Display RMON history</td>
<td>`display rmon history [interface-type</td>
<td></td>
</tr>
<tr>
<td>information</td>
<td>interface-number</td>
<td>unit</td>
</tr>
<tr>
<td>Display RMON alarm</td>
<td><code>display rmon alarm [entry-number ]</code></td>
<td></td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display extended RMON</td>
<td><code>display rmon prialarm [prialarm-entry-number]</code></td>
<td></td>
</tr>
<tr>
<td>alarm information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display RMON events</td>
<td><code>display rmon event [event-entry ]</code></td>
<td></td>
</tr>
<tr>
<td>Display RMON event logs</td>
<td><code>display rmon eventlog [event-entry ]</code></td>
<td></td>
</tr>
</tbody>
</table>

### RMON Configuration Examples

#### Network requirements

- The switch to be tested is connected to a remote NMS through the Internet. Ensure that the SNMP agents are correctly configured before performing RMON configuration.

- Create an entry in the extended alarm table to monitor the information of statistics on the Ethernet port, if the change rate of which exceeds the set threshold, the alarm events will be triggered.

#### Network diagram

**Figure 233** Network diagram for RMON configuration

![Network diagram](image)

#### Configuration procedures

```
# Add the statistics entry numbered 1 to take statistics on Ethernet 1/0/1.
<5500> system-view
[5500] interface Ethernet 1/0/1
```
RMON Configuration Examples

[5500-Ethernet1/0/1] rmon statistics 1
[5500-Ethernet1/0/1] quit

# Add the event entries numbered 1 and 2 to the event table, which will be triggered by the following extended alarm.

[5500] rmon event 1 log
[5500] rmon event 2 trap 10.21.30.55

# Add an entry numbered 2 to the extended alarm table to allow the system to calculate the alarm variables with the (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) formula to get the numbers of all the oversize and undersize packets received by Ethernet 1/0/1 that are in correct data format and sample it in every 10 seconds. When the change ratio between samples reaches the rising threshold of 50, event 1 is triggered; when the change ratio drops under the falling threshold, event 2 is triggered.

[5500] rmon prialarm 2 (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)
  test 10 changeratio rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1

# Display the RMON extended alarm entry numbered 2.

[5500] display rmon prialarm 2
Prialarm table 2 owned by user1 is VALID.
  Samples type : changeratio
  Variable formula : (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)
  Description : test
  Sampling interval : 10(sec)
  Rising threshold : 100(linked with event 1)
  Falling threshold : 10(linked with event 2)
  When startup enables : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value : 0
Network Time Protocol (NTP) is a time synchronization protocol defined in RFC 1305. It is used for time synchronization between a set of distributed time servers and clients. Carried over UDP, NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications (See “Applications of NTP”).

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP messages.

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control (See “Configuring Access Control Right” on page 819) and MD5 encrypted authentication (See “Configuring NTP Authentication” on page 820)
- Sending protocol packets in unicast, multicast, or broadcast mode
The clock stratum determines the accuracy, which ranges from 1 to 16. The stratum of a reference clock ranges from 1 to 15. The clock accuracy decreases as the stratum number increases. A stratum 16 clock is in the unsynchronized state and cannot serve as a reference clock.

The local clock of a Switch 5500 cannot be set as a reference clock. It can serve as a reference clock source to synchronize the clock of other devices only after it is synchronized.

Implementation Principle of NTP

Figure 234 shows the implementation principle of NTP. Ethernet switch A (Device A) is connected to Ethernet switch B (Device B) through Ethernet ports. Both having their own system clocks, they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of Device A and Device B are synchronized, the clock of Device A is set to 10:00:00 am, and the clock of Device B is set to 11:00:00 am.
- Device B serves as the NTP server, that is, the clock of Device A will be synchronized to that of Device B.
- It takes one second to transfer an NTP message from Device A to Device B or from Device B to Device A.
- When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

The procedure of synchronizing the system clock is as follows:
- Device A sends an NTP message to Device B, with a timestamp 10:00:00 am \((T_1)\) identifying when it is sent.
- When the message arrives at Device B, Device B inserts its own timestamp 11:00:01 am \((T_2)\) into the packet.
- When the NTP message leaves Device B, Device B inserts its own timestamp 11:00:02 am \((T_3)\) into the packet.
- When receiving a response packet, Device A inserts a new timestamp 10:00:03 am \((T_4)\) into it.

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:
  \[
  \text{Delay} = (T_4 - T_1) - (T_3 - T_2).
  \]
- Time offset of Device A relative to Device B:
  \[
  \text{Offset} = ((T_2 - T_1) + (T_3 - T_4))/2.
  \]

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

For detailed information, refer to RFC 1305.

**NTP Implementation Modes**

According to the network structure and the position of the local Ethernet switch in the network, the local Ethernet switch can work in multiple NTP modes to synchronize the clock.

**Server/client mode**

*Figure 235  Server/client mode*
Symmetric peer mode

Figure 236 Symmetric peer mode

In the symmetric peer mode, the local Switch 5500 serves as the symmetric-active peer and sends clock synchronization request first, while the remote server serves as the symmetric-passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

Broadcast mode

Figure 237 Broadcast mode

In broadcast mode, the server initiates a client/server mode request after receiving the first broadcast packet. The client obtains the delay between the client and server and works in the broadcast client mode. The client receives broadcast packets and synchronizes the local clock.

Multicast mode

Figure 238 Multicast mode

In multicast mode, the server initiates a client/server mode request after receiving the first multicast packet. The client obtains the delay between the client and server and works in the multicast client mode. The client receives multicast packets and synchronizes the local clock.
Table 608 describes how the above mentioned NTP modes are implemented on the 3Com Switch 5500 Family.

Table 608  NTP implementation modes on the 3Com Switch 5500 Family

<table>
<thead>
<tr>
<th>NTP implementation mode</th>
<th>Configuration on the Switch 5500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/client mode</td>
<td>Configure the local Switch 5500 to work in the NTP client mode. In this mode, the remote server serves as the local time server, while the local switch serves as the client.</td>
</tr>
<tr>
<td>Symmetric peer mode</td>
<td>Configure the local Switch 5500 to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the Switch 5500, and the local switch serves as the symmetric-active peer.</td>
</tr>
<tr>
<td>Broadcast mode</td>
<td>Configure the local Switch 5500 to work in NTP broadcast server mode. In this mode, the local switch broadcasts NTP messages through the VLAN interface configured on the switch. Configure the Switch 5500 to work in NTP broadcast client mode. In this mode, the local Switch 5500 receives broadcast NTP messages through the VLAN interface configured on the switch.</td>
</tr>
<tr>
<td>Multicast mode</td>
<td>Configure the local Switch 5500 to work in NTP multicast server mode. In this mode, the local switch sends multicast NTP messages through the VLAN interface configured on the switch. Configure the local Switch 5500 to work in NTP multicast client mode. In this mode, the local switch receives multicast NTP messages through the VLAN interface configured on the switch.</td>
</tr>
</tbody>
</table>

**CAUTION:**

- *When the Switch 5500 is in server mode or symmetric passive mode, you need not perform related configurations on this switch, but on the client or the symmetric-active peer.*

- *The NTP server mode, NTP broadcast mode, or NTP multicast mode takes effect only after the local clock of the 3Com Switch 5500 has been synchronized.*

- *When symmetric peer mode is configured on two Ethernet switches, to synchronize the clock of the two switches, make sure at least one switch’s clock has been synchronized.*

Table 609  NTP configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Configuring NTP Implementation Modes&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring Access Control Right&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring NTP Authentication&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Optional NTP Parameters&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Displaying NTP Configuration&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>
CHAPTER 70: NTP CONFIGURATION

Configuring NTP Implementation Modes

A Switch 5500 can work in one of the following NTP modes:

- “Configuring NTP Server/Client Mode”
- “Configuring the NTP Symmetric Peer Mode”
- “Configuring NTP Broadcast Mode”
- “Configuring NTP Multicast Mode”

To protect unused sockets against attacks by malicious users and improve security, the 3Com Switch 5500 Family provides the following functions:

- UDP port 123 is opened only when the NTP feature is enabled.
- UDP port 123 is closed as the NTP feature is disabled.

These functions are implemented as follows:

- Execution of one of the ntp-service unicast-server, ntp-service unicast-peer, ntp-service broadcast-client, ntp-service broadcast-server, ntp-service multicast-client, and ntp-service multicast-server commands enables the NTP feature and opens UDP port 123 at the same time.
- Execution of the undo form of one of the above six commands disables all implementation modes of the NTP feature and closes UDP port 123 at the same time.

Configuring NTP Server/Client Mode

For switches working in the server/client mode, you only need to perform configurations on the clients, and not on the servers.

Table 610 Configure an NTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure an NTP client</td>
<td>ntp-service unicast-server {</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>remote-ip</td>
<td>server-name } [</td>
</tr>
<tr>
<td></td>
<td>authentication-keyid key-id ] [</td>
<td></td>
</tr>
<tr>
<td></td>
<td>priority</td>
<td>source-interface ]</td>
</tr>
<tr>
<td></td>
<td>Vlan-interface vlan-id</td>
<td>version number ]*</td>
</tr>
</tbody>
</table>

- The remote server specified by remote-ip or server-name serves as the NTP server, and the local switch serves as the NTP client. The clock of the NTP client will be synchronized by but will not synchronize that of the NTP server.
- remote-ip cannot be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the source-interface keyword, the source IP address of the NTP message will be configured as the primary IP address of the specified interface.
- A switch can act as a server to synchronize the clock of other switches only after its clock has been synchronized. If the clock of a server has a stratum level lower 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 client will choose the optimal reference source.
Configuring the NTP Symmetric Peer Mode

For switches working in the symmetric peer mode, you need to specify a symmetric-passive peer on the symmetric-active peer.

Table 611 Configure a symmetric-active switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify a symmetric-passive peer for the switch</td>
<td>ntp-service unicast-peer {remote-ip</td>
<td>peer-name} [authentication-keyid key-id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a switch is not configured to work in the symmetric mode.</td>
</tr>
</tbody>
</table>

- In the symmetric peer mode, you need to execute the related NTP configuration commands (refer to “Configuring NTP Implementation Modes” for details) to enable NTP on a symmetric-passive peer; otherwise, the symmetric-passive peer will not process NTP messages from the symmetric-active peer.

- The remote device specified by remote-ip or peer-name serves as the peer of the local Ethernet switch, and the local switch works in the symmetric-active mode. In this case, the clock of the local switch and that of the remote device can be synchronized to each other.

- remote-ip must not be a broadcast address, a multicast address or the IP address of the local clock.

- After you specify an interface for sending NTP messages through the source-interface keyword, the source IP address of the NTP message will be configured as the IP address of the specified interface.

- Typically, the clock of at least one of the symmetric-active and symmetric-passive peers should be synchronized first; otherwise the clock synchronization will not proceed.

- You can configure multiple symmetric-passive peers for the local switch by repeating the ntp-service unicast-peer command. The clock of the peer with the smallest stratum will be chosen to synchronize with the local clock of the switch.

Configuring NTP Broadcast Mode

For switches working in the broadcast mode, you need to configure both the server and clients. The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. The switches working in the NTP broadcast client mode will respond to the NTP messages, so as to start the clock synchronization.

A 3Com Switch 5500 can operate as a broadcast server or a broadcast client.

- Refer to Table 612 for configuring a switch to work in the NTP broadcast server mode.

- Refer to Table 613 for configuring a switch to work in the NTP broadcast client mode.

A broadcast server can synchronize broadcast clients only after its clock has been synchronized.
Configuring a switch to work in the NTP broadcast server mode

Table 612 Configure a switch to work in the NTP broadcast server mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface</td>
<td>-</td>
</tr>
<tr>
<td>Configure the switch to work in the NTP broadcast server mode</td>
<td>ntp-service broadcast-server [ authentication-keyid key-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>[ version number ]*</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a switch to work in the NTP broadcast client mode

Table 613 Configure a switch to work in the NTP broadcast client mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface</td>
<td>-</td>
</tr>
<tr>
<td>Configure the switch to work in the NTP broadcast client mode</td>
<td>ntp-service broadcast-client</td>
<td>Required</td>
</tr>
</tbody>
</table>

Configuring NTP Multicast Mode

For switches working in the multicast mode, you need to configure both the server and clients. The multicast server periodically sends NTP multicast messages to multicast clients. The switches working in the NTP multicast client mode will respond to the NTP messages, so as to start the clock synchronization.

A 3Com Switch 5500 can work as a multicast server or a multicast client.

- Refer to Table 614 for configuring a switch to work in the NTP multicast server mode.
- Refer to Table 615 for configuring a switch to work in the NTP multicast client mode.

A multicast server can synchronize multicast clients only after its clock has been synchronized.

The Switch 5500 working in the multicast server mode supports up to 1,024 multicast clients.

Configuring a switch to work in the multicast server mode

Table 614 Configure a switch to work in the NTP multicast server mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface</td>
<td>-</td>
</tr>
<tr>
<td>Configure the switch to work in the NTP multicast server mode</td>
<td>ntp-service multicast-server [ ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>] [ [ authentication-keyid keyid ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>] [ ttl ttl-number ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ version number ]*</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a switch to work in the multicast client mode

Table 615  Configure a switch to work in the NTP multicast client mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure the switch to work in the NTP multicast client mode</td>
<td>ntp-service multicast-client [ ip-address ]</td>
<td>Required Not configured by default.</td>
</tr>
</tbody>
</table>

Configuring Access Control Right

With the following command, you can configure the NTP service access-control right to the local switch for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called control query refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.

- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.

- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.

- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the 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 in this order and use the first matched right.

Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local switch for peer devices, you need to create and configure an ACL associated with the access-control right. To configure an ACL, refer to “ACL Configuration” on page 663.

Configuration Procedure

Table 616  Configure the NTP service access-control right to the local device for peer devices

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the NTP service access-control right to the local switch for peer devices</td>
<td>ntp-service access { peer</td>
<td>server</td>
</tr>
</tbody>
</table>

Configuration

Prerequisites

With the following command, you can configure the NTP service access-control right to the local switch for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called control query refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.

- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.

- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.

- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the 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 in this order and use the first matched right.

Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local switch for peer devices, you need to create and configure an ACL associated with the access-control right. To configure an ACL, refer to “ACL Configuration” on page 663.

Configuration Procedure

Table 616  Configure the NTP service access-control right to the local device for peer devices

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the NTP service access-control right to the local switch for peer devices</td>
<td>ntp-service access { peer</td>
<td>server</td>
</tr>
</tbody>
</table>
The access-control right mechanism provides only a minimum degree of security protection for the local switch. A more secure method is identity authentication.

### Configuring NTP Authentication

In networks with higher security requirements, the NTP authentication function must be enabled to run NTP. Through password authentication on the client and the server, the clock of the client is synchronized only to that of the server that passes the authentication. This improves network security. Table 617 shows the roles of devices in the NTP authentication function.

<table>
<thead>
<tr>
<th>Role of device</th>
<th>Working mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Client in the server/client mode</td>
</tr>
<tr>
<td></td>
<td>Client in the broadcast mode</td>
</tr>
<tr>
<td></td>
<td>Client in the multicast mode</td>
</tr>
<tr>
<td></td>
<td>Symmetric-active peer in the symmetric peer mode</td>
</tr>
<tr>
<td>Server</td>
<td>Server in the server/client mode</td>
</tr>
<tr>
<td></td>
<td>Server in the broadcast mode</td>
</tr>
<tr>
<td></td>
<td>Server in the multicast mode</td>
</tr>
<tr>
<td></td>
<td>Symmetric-passive peer in the symmetric peer mode</td>
</tr>
</tbody>
</table>

### Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the clock of the client can be synchronized to a server no matter whether the NTP authentication function is enabled on the server (assuming that other related configurations are properly performed).
- For the NTP authentication function to take effect, a trusted key needs to be configured on both the client and server after the NTP authentication is enabled on them.
- The local clock of the client is only synchronized to the server that provides a trusted key.
- In addition, for the server/client mode and the symmetric peer mode, you need to associate a specific key on the client (the symmetric-active peer in the symmetric peer mode) with the corresponding NTP server (the symmetric-passive peer in the symmetric peer mode); for the NTP broadcast/multicast mode, you need to associate a specific key on the broadcast/multicast server with the corresponding NTP broadcast/multicast client. Otherwise, NTP authentication cannot be enabled normally.
- Configurations on the server and the client must be consistent.
Configuring NTP Authentication

Configuring NTP Authentication on the Client

Table 618 Configure NTP authentication on the client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the NTP authentication function</td>
<td>ntp-service authentication enable</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;Disabled by default.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Configure the NTP authentication key</td>
<td>ntp-service authentication-keyid key-id</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;By default, no NTP authentication key is configured.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Configure the specified key as a trusted key</td>
<td>ntp-service reliable authentication-keyid key-id</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;By default, no trusted key is configured.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Associate the specified key with the corresponding NTP server</td>
<td>ntp-service unicast-server {&lt;br&gt;   remote-ip</td>
<td>server-name&lt;br&gt;   authentication-keyid key-id&lt;br&gt;   authentication-model md5 value}&lt;br&gt;ntp-service unicast-peer {&lt;br&gt;   remote-ip</td>
</tr>
</tbody>
</table>

NTP authentication requires that the authentication keys configured for the server and the client be the same. Besides, the authentication keys must be trusted keys. Otherwise, the clock of the client cannot be synchronized with that of the server.

Configuring NTP Authentication on the Server

Table 619 Configure NTP authentication on the server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable NTP authentication</td>
<td>ntp-service authentication enable</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;Disabled by default.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Configure an NTP authentication key</td>
<td>ntp-service authentication-keyid key-id</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;By default, no NTP authentication key is configured.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Configure the specified key as a trusted key</td>
<td>ntp-service reliable authentication-keyid key-id</td>
<td>- Requirement&lt;ul&gt;&lt;li&gt;By default, no trusted key is configured.&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
<td>-</td>
</tr>
</tbody>
</table>
The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

### Configuring Optional NTP Parameters

#### Configuring an Interface on the Local Switch to Send NTP messages

Table 619 Configure NTP authentication on the server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Associate the specified key with the corresponding broadcast/multicast client | Configure on the NTP broadcast server ntp-service broadcast-server authentication-keyid key-id | - In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client.
| Configure on the NTP multicast server ntp-service multicast-server authentication-keyid key-id | You can associate an NTP broadcast/multicast client with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode. |

#### Configuring the Number of Dynamic Sessions Allowed on the Local Switch

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.

#### Configuring Optional NTP Parameters

Table 620 Optional NTP parameters configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring an Interface on the Local Switch to Send NTP messages”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Configuring the Number of Dynamic Sessions Allowed on the Local Switch”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Disabling an Interface from Receiving NTP Messages”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

#### Configuring an Interface on the Local Switch to Send NTP messages

Table 621 Configure an interface on the local switch to send NTP messages

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure an interface on the local switch to send NTP messages</td>
<td>ntp-service source-interface Vlan-interface vlan-id</td>
<td>Required</td>
</tr>
</tbody>
</table>

**CAUTION:** If you have specified an interface in the ntp-service unicast-server or ntp-service unicast-peer command, this interface will be used for sending NTP messages.
In the server/client 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.

<table>
<thead>
<tr>
<th>Table 622</th>
<th>Configure the number of dynamic sessions allowed on the local switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Configure the maximum number of dynamic sessions that can be established on the local switch</td>
<td>ntp-service max-dynamic-sessions number</td>
</tr>
</tbody>
</table>

Disabling an Interface from Receiving NTP Messages

<table>
<thead>
<tr>
<th>Table 623</th>
<th>Disable an interface from receiving NTP messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface Vlan-interface vlan-id</td>
</tr>
<tr>
<td>Disable an interface from receiving NTP messages</td>
<td>ntp-service in-interface disable</td>
</tr>
</tbody>
</table>

Displaying NTP Configuration

After completing the above configuration, you can execute the `display` commands in any view to display the running status of switch, and verify the effect of the configurations.

<table>
<thead>
<tr>
<th>Table 624</th>
<th>Display NTP configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Display the status of NTP services</td>
<td>display ntp-service status</td>
</tr>
<tr>
<td>Display the information about the sessions maintained by NTP</td>
<td>display ntp-service sessions [ verbose ]</td>
</tr>
<tr>
<td>Display the brief information about NTP servers along the path from the local device to the reference clock source</td>
<td>display ntp-service trace</td>
</tr>
</tbody>
</table>
**Configuration Example**

### Configuring NTP Server/Client Mode

**Network requirements**
- The local clock of Device A (a switch) is to be used as a master clock, with the stratum level of 2.
- Device A is used as the NTP server of Device B (a Switch 5500)
- Configure Device B to work in the client mode, and then Device A will automatically work in the server mode.

**Network diagram**

*Figure 239* Network diagram for the NTP server/client mode configuration

![Network Diagram]

**Configuration procedure**

Perform the following configurations on Device B.

# View the NTP status of Device B before synchronization.

```
<DeviceB> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
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)
```

# Set Device A as the NTP server of Device B.

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

# (After completing the above configuration, Device B is synchronized to Device A.) View the NTP status of Device B.

```
[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
```
Peer dispersion: 9.63 ms  
Reference time: 17:03:32.022 UTC Thu Apr 7 2007 (BF422AE4.05AEA86C)

The above output information indicates that Device B is synchronized to Device A, and the stratum level of its clock is 3, one level lower than that of Device A.

# View the information about NTP sessions of Device B. (You can see that Device B establishes a connection with Device A.)

[DeviceB] display ntp-service sessions

<table>
<thead>
<tr>
<th>source</th>
<th>reference</th>
<th>stratum</th>
<th>reach</th>
<th>poll</th>
<th>now</th>
<th>offset</th>
<th>delay</th>
<th>disper</th>
</tr>
</thead>
<tbody>
<tr>
<td>12345</td>
<td>1.0.1.11</td>
<td>127.127.1.0</td>
<td>2</td>
<td>1</td>
<td>64</td>
<td>1</td>
<td>350.1</td>
<td>15.1</td>
</tr>
</tbody>
</table>

note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured
Total associations: 1

---

### Configuring NTP

#### Symmetric Peer Mode

**Network requirements**

- The local clock of Device A is set as the NTP master clock, with the clock stratum level of 2.
- Device C (a Switch 5500) uses Device A as the NTP server, and Device A works in server mode automatically.
- The local clock of Device B is set as the NTP master clock, with the clock stratum level of 1. Set Device C as the peer of Device B.

#### Network diagram

**Figure 240** Network diagram for NTP peer mode configuration

---

**Configuration procedure**

1. Configure Device C.
   
   # Set Device A as the NTP server.
   
   <DeviceC> system-view
   
   [DeviceC] ntp-service unicast-server 3.0.1.31

2. Configure Device B (after the Device C is synchronized to Device A).
   
   # Enter system view.
   
   <DeviceB> system-view
   
   # Set Device C as the peer of Device B.
   
   [DeviceB] ntp-service unicast-peer 3.0.1.33
Device C and Device B are symmetric peers after the above configuration. Device B works in symmetric active mode, while Device C works in symmetric passive mode. Because the stratum level of the local clock of Device B is 1, and that of Device C is 3, the clock of Device C is synchronized to that of Device B.

View the status of Device C after the clock synchronization.

```plaintext
[DeviceC] display ntp-service status
Clock status: synchronized
Clock stratum: 2
Reference clock ID: 3.0.1.32
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu APR 7 2007 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device C is synchronized to that of Device B and the stratum level of its local clock is 2, one level lower than Device B.

# View the information about the NTP sessions of Device C (you can see that a connection is established between Device C and Device B).

```plaintext
[DeviceC] display ntp-service sessions
source reference stratum reach poll now offset delay disper
*************************************************************************
[1234] 3.0.1.32 LOCL 1 95 64 42 -14.3 12.9 2.7
[25] 3.0.1.31 127.127.1.0 2 1 64 1 4408.6 38.7 0.0
note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured
Total associations : 2
```

### Configuring NTP

**Broadcast Mode**

- The local clock of Device C is set as the NTP master clock, with a stratum level of 2. Configure Device C to work in the NTP broadcast server mode and send NTP broadcast messages through VLAN-interface 2.

- Device A and Device D are two Switch 5500s. Configure Device A and Device D to work in the NTP broadcast client mode and listen to broadcast messages through their own VLAN-interface 2.
**Network diagram**

*Figure 241* Network diagram for the NTP broadcast mode configuration

---

**Configuration procedure**

1. Configure Device C.
   
   # Enter system view.
   
   ```
   <DeviceC> system-view
   ``
   
   # Set Device C as the broadcast server, which sends broadcast messages through VLAN-interface 2.
   
   ```
   [DeviceC] interface Vlan-interface 2
   [DeviceC-Vlan-interface2] ntp-service broadcast-server
   ```

2. Configure Device A. (perform the same configuration on Device D)
   
   # Enter system view.
   
   ```
   <DeviceA> system-view
   ``
   
   # Set Device A as a broadcast client.
   
   ```
   [DeviceA] interface Vlan-interface 2
   [DeviceA-Vlan-interface2] ntp-service broadcast-client
   ```

After completing the above configuration, Device A and Device D will listen to broadcast messages through their own VLAN-interface 2, and Device C will send broadcast messages through VLAN-interface 2. Because Device A and Device C do not share the same network segment, Device A cannot receive broadcast messages from Device C, while Device D is synchronized to Device C after receiving broadcast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
```
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AE4.05AEA86C)

The output information indicates that Device D is synchronized to Device C, with the clock stratum level of 3, one level lower than that of Device C.

# View the information about the NTP sessions of Device D and you can see that a connection is established between Device D and Device C.

[DeviceD] display ntp-service sessions
source reference stratum reach poll now offset delay dispersion
**************************************************************************
[1234] 3.0.1.31 127.127.1.0 2 1 64 377 26.1 199.53 9.7
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 Device C is set as the NTP master clock, with a clock stratum level of 2. Configure Device C to work in the NTP multicast server mode and advertise multicast NTP messages through VLAN-interface2.
- Device A and Device D are two Switch 5500s. Configure Device A and Device D to work in the NTP multicast client mode and listen to multicast messages through their own VLAN-interface2.

Network diagram

Figure 242  Network diagram for NTP multicast mode configuration

Configuration procedure
1 Configure Device C.
   # Enter system view.
   <DeviceC> system-view
   # Set Device C as a multicast server to send multicast messages through VLAN-interface2.
   [DeviceC] interface Vlan-interface 2
   [DeviceC-Vlan-interface2] ntp-service multicast-server
2 Configure Device A (perform the same configuration on Device D).
   # Enter system view.
<DeviceA> system-view
# Set Device A as a multicast client to listen to multicast messages through VLAN-interface2.
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service multicast-client

After completing the above configuration, Device A and Device D respectively listen to multicast messages through their own VLAN-interface2, and Device C advertises multicast messages through VLAN-interface2. Because Device A and Device C do not share the same network segment, Device A cannot receive multicast messages from Device C, while Device D is synchronized to Device C after receiving multicast messages from Device C.

View the NTP status of Device D after the clock synchronization.

[DeviceD] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 7 2006 (BF422AB4.05ABA86C)

The output information indicates that Device D is synchronized to Device C, with a clock stratum level of 3, one stratum level lower than that of Device C.

# View the information about the NTP sessions of Device D (You can see that a connection is established between Device D and Device C).

[DeviceD] display ntp-service sessions
source reference stra reach poll now offset delay disper
**************************************************************************
[1234]3.0.1.31 127.127.1.0 2 1 64 377 26.1 199.53 9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured To
tal associations : 1

Configuring NTP Server/Client Mode with Authentication

Network requirements
■ The local clock of Device A is set as the NTP master clock, with a clock stratum level of 2.
■ Device B is a Switch 5500 and uses Device A as the NTP server. Device B is set to work in client mode, while Device A works in server mode automatically.
■ The NTP authentication function is enabled on Device A and Device B.

Network diagram

Figure 243 Network diagram for NTP server/client mode with authentication configuration
Configuration procedure

1 Configure Device B.
   # Enter system view.
   <DeviceB> system-view
   # Enable the NTP authentication function.
   [DeviceB] ntp-service authentication enable
   # Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.
   [DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
   # Specify the key 42 as a trusted key.
   [DeviceB] ntp-service reliable authentication-keyid 42
   # Associate the trusted key with the NTP server (Device A).
   [DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42

After completing the above configuration, Device B is ready to synchronize with Device A. Because the NTP authentication function is not enabled on Device A, the clock of Device B will fail to be synchronized to that of Device A.

2 To synchronize Device B, you need to perform the following configurations on Device A.
   # Enable the NTP authentication function.
   <DeviceA> system-view
   [DeviceA] ntp-service authentication enable
   # Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.
   [DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
   # Specify the key 42 as a trusted key.
   [DeviceA] ntp-service reliable authentication-keyid 42

   (After completing the above configuration, the clock of Device B can be synchronized to that of Device A.) View the status of Device B after synchronization.

   [DeviceB] display ntp-service status
   Clock status: synchronized
   Clock stratum: 3
   Reference clock ID: 1.0.1.11
   Nominal frequence: 100.0000 Hz
   Actual frequence: 100.1000 Hz
   Clock precision: 2^18
   Clock offset: 0.66 ms
   Root delay: 27.47 ms
   Root dispersion: 208.39 ms
   Peer dispersion: 9.63 ms
   Reference time: 17:03:32.022 UTC Thu Apr 7 2007 (BF422AE4.05AEA86C)

The output information indicates that the clock of Device B is synchronized to that of Device A, with a clock stratum level of 3, one stratum level lower than that of Device A.
# View the information about NTP sessions of Device B (you can see that a connection is established between Device B and Device A).

```plaintext
<DeviceB> display ntp-service sessions

source reference stra reach poll now offset delay disper
*************************************************************************
1.0.1.11 127.127.1.0 2 255 64 8 2.8 17.7 1.2

note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured
Total associations : 1
```
SSH Overview

**Introduction to SSH**
Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments. In an SSH connection, data are encrypted before being sent out and decrypted after they reach the destination. This prevents attacks such as plain text password interception. Besides, SSH also provides powerful user authentication functions that prevent attacks such as DNS and IP spoofing.

SSH adopts the client-server model. The device can be configured as an SSH client or an SSH server. In the former case, the device establishes a remote SSH connection to an SSH server. In the latter case, the device provides connections to multiple clients.

Furthermore, SSH can also provide data compression to increase transmission speed, take the place of Telnet or provide a secure channel for FTP.

*CAUTION: Currently, device supports only SSH2.*

**Algorithm and Key**
Algorithm is a set of transformation rules for encryption and decryption. Information without being encrypted is known as plain text, while information that is encrypted is known as cipher text. Encryption and decryption are performed using a string of characters called a key, which controls the transformation between plain text and cipher text, for example, changing the plain text into cipher text or cipher text into plain text.

![Encryption and decryption](image)

Key-based algorithm is usually classified into symmetric key algorithm and asymmetric key algorithm.

**Asymmetric Key Algorithm**
Asymmetric key algorithm means that a key pair exists at both ends. The key pair consists of a private key and a public key. The public key is effective for both ends, while the private key is effective only for the local end. Normally you cannot use the private key through the public key.
Asymmetric key algorithm encrypts data using the public key and decrypts the data using the private key, thus ensuring data security.

You can also use the asymmetric key algorithm for data signature. For example, user 1 adds his 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, this means that the data originates from user 1.

Both Revest-Shamir-Adleman Algorithm (RSA) and Digital Signature Algorithm (DSA) are asymmetric key algorithms. RSA is used for data encryption and signature, whereas DSA is used for adding signature.

Currently, SSH supports both RSA and DSA.

### SSH Operating Process

The session establishment between an SSH client and the SSH server involves the following five stages:

**Table 625  Stages in establishing a session between the SSH client and server**

<table>
<thead>
<tr>
<th>Stages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version negotiation</td>
<td>The two parties negotiate a version to use.</td>
</tr>
<tr>
<td>Key and algorithm negotiation</td>
<td>SSH supports multiple algorithms. The two parties negotiate an algorithm for communication.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The SSH server authenticates the client in response to the client’s authentication request.</td>
</tr>
<tr>
<td>Session request</td>
<td>This client sends a session request to the server.</td>
</tr>
<tr>
<td>Data exchange</td>
<td>The client and the server start to communicate with each other.</td>
</tr>
</tbody>
</table>

**Version negotiation**

- The server opens port 22 to listen to connection requests from clients.
- 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.
- 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.
- 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 to determine whether it can cooperate with the client.
- If the negotiation is successful, the server and the client go on to the key and algorithm negotiation. If not, the server breaks the TCP connection.

- All the packets above are transferred in plain text.
Key negotiation

- The server and the client send algorithm negotiation packets to each other, which contain public key algorithm lists supported by the server and the client, encrypted algorithm list, message authentication code (MAC) algorithm list, and compressed algorithm list.
- The server and the client calculate the final algorithm according to the algorithm lists supported.
- The server and the client generate the session key and session ID based on the Diffie-Hellman (DH) exchange algorithm and the host key pair.
- Then, the server and the client get the same session key and use it for data encryption and decryption to secure data communication.

Authentication negotiation

The negotiation steps are as follows:

- The client sends an authentication request to the server. The authentication request contains username, authentication type, and authentication-related information. For example, if the authentication type is password, the content is the password.
- The server starts to authenticate the user. If authentication fails, the server sends an authentication failure message to the client, which contains the list of methods used for a new authentication process.
- The client selects an authentication type from the method list to perform authentication again.
- The above process repeats until the authentication succeeds, or the connection is torn down when the authentication times reach the upper limit.

SSH provides two authentication methods: password authentication and publickey authentication.

- In password authentication, the client encrypts the 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, compares them with those it maintains, and then informs the client of the authentication result.
- The publickey authentication method authenticates clients using digital signatures. Currently, the device supports two publickey algorithms to implement digital signatures: RSA and DSA. The client sends to the server a publickey authentication request containing its user name, public key and algorithm. The server verifies the public key. If the public key is invalid, the authentication fails; otherwise, the server generates a digital signature to authenticate the client, and then sends back a message to inform the success or failure of the 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. If the client passes authentication, 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. The client sends a session request to the server, which processes the request and establishes a session.

**Data exchange**

In this stage, the server and the client exchanges data in this 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.

### Configuring the SSH Server

You must perform necessary configurations on the SSH server for SSH clients to access.

#### SSH Server Configuration Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the SSH server</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring the User Interfaces for SSH Clients</td>
<td>Required</td>
</tr>
<tr>
<td>Creating/Deleting a Key Pair</td>
<td>Optional</td>
</tr>
<tr>
<td>Exporting the RSA or DSA Public Key</td>
<td>Optional</td>
</tr>
<tr>
<td>Creating an SSH User and Specify an Authentication Type</td>
<td>Required</td>
</tr>
<tr>
<td>Specifying a Service Type for an SSH User</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring SSH Management</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring the Client Public Key on the Server</td>
<td>Required for <strong>publickey</strong> authentication; unnecessary for <strong>password</strong> authentication</td>
</tr>
<tr>
<td>Assigning a Public Key to an SSH User</td>
<td>Required for <strong>publickey</strong> authentication; unnecessary for <strong>password</strong> authentication</td>
</tr>
<tr>
<td>Specifying a Source IP Address/Interface for the SSH Server</td>
<td>Optional</td>
</tr>
</tbody>
</table>

#### 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 the SSH clients to allow an SSH login. This configuration takes effect at the next login.

### Table 627  Configure the protocol(s) that a user interface supports

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter user interface view of one or multiple user interfaces</td>
<td>user-interface vty first-number [ last-number ]</td>
<td>-</td>
</tr>
<tr>
<td>Configure the authentication mode as scheme</td>
<td>authentication-mode scheme [ command-authorization ]</td>
<td>Required by default, the user interface authentication mode is password</td>
</tr>
</tbody>
</table>
CAUTION:

- If you have configured a user interface to support SSH protocol, you must configure AAA authentication for the user interface by using the `authentication-mode scheme` command to ensure successful login.
- On a user interface, if the `authentication-mode password` or `authentication-mode none` command has been executed, the `protocol inbound ssh` command is not available. Similarly, if the `protocol inbound ssh` command has been executed, the `authentication-mode password` and `authentication-mode none` commands are not available.

### Generating/Destroying a RSA or DSA Key Pair

This configuration task lets you generate or destroy a key pair. You must generate an RSA and a DSA key pair on the server for an SSH client to log in successfully. When generating a key pair, you will be prompted to enter the key length in bits, which is between 512 and 2048. The default length is 1024. If a key pair already exists, the system prompts you to indicate whether to replace the existing key pair.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>Required</td>
</tr>
<tr>
<td>Generate an RSA key pair</td>
<td><code>public-key local create rsa</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no RSA key pair is created.</td>
</tr>
<tr>
<td>Destroy the RSA key pair</td>
<td><code>public-key local destroy rsa</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the command to destroy the configured RSA key pair.</td>
</tr>
<tr>
<td>Generate a DSA key pair</td>
<td><code>public-key local create dsa</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no DSA key pair is created.</td>
</tr>
<tr>
<td>Destroy the DSA key pair</td>
<td><code>public-key local destroy dsa</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the command to destroy the configured DSA key pair.</td>
</tr>
</tbody>
</table>

- The command for generating a key pair can survive a reboot. You only need to configure it once.
- For a fabric made up of multiple devices, you need to create the key pairs on the management device to ensure that all devices in the fabric have the same local RSA key pairs.
- Some third-party software, for example, WinSCP, requires that the modulo of a public key be greater than or equal to 768. Therefore, a local key pair of more than 768 bits is recommended.
Exporting the RSA or DSA Public Key

You can display the generated RSA or DSA key pair on the screen in a specified format, or export it to a specified file for configuring the key at a remote end.

<table>
<thead>
<tr>
<th>Table 629</th>
<th>Export the RSA public key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Display the RSA key on the screen in a specified format or export it to a specified file</td>
<td>public-key local export rsa { openssh</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 630</th>
<th>Export the DSA public key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Display the DSA key on the screen in a specified format or export it to a specified file</td>
<td>public-key local export dsa { openssh</td>
</tr>
</tbody>
</table>

The DSA public key format can be SSH2 and OpenSSH, while the RSA public key format can be SSH1, SSH2 and OpenSSH.

Creating an SSH User and Specify an Authentication Type

This task is to create an SSH user and specify an authentication type for it. Specifying an authentication type for a new user is a must to get the user login.

<table>
<thead>
<tr>
<th>Table 631</th>
<th>Configure an SSH user and specify an authentication type for it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>sshAuthentication-type</td>
</tr>
<tr>
<td>Specify the default authentication type for all SSH users</td>
<td>default { all</td>
</tr>
<tr>
<td>Create an SSH user, and specify an authentication type for it</td>
<td>ssh user username authentication-type { all</td>
</tr>
</tbody>
</table>

CAUTION:

- For password authentication type, the username argument must be consistent with the valid user name defined in AAA; for publickey authentication, the username argument is the SSH local user name, so that there is no need to configure a local user in AAA.

- If the default authentication type for SSH users is password and local AAA authentication is adopted, you need not use the ssh user command to create an SSH user. Instead, you can use the local-user command to create a user name and its password and then set the service type of the user to SSH.

- If the default authentication type for SSH users is password and remote authentication (RADIUS authentication, for example) is adopted, you need not use the ssh user command to create an SSH user, because it is created on the
remote server. And the user can use its username and password configured on
the remote server to access the network.

- Under the **publickey** authentication mode, the level of commands available to
  a logged-in SSH user can be configured using the **user privilege level**
  command on the server, and all the users with this authentication mode will
  enjoy this level.

- Under the **password** or **password-publickey** authentication mode, the level
  of commands available to a logged-in SSH user is determined by the AAA
  scheme. Meanwhile, for different users, the available levels of commands are
  also different.

- Under the **all** authentication mode, the level of commands available to a
  logged-in SSH user is determined by the actual authentication method used for
  the user.

### Specifying a Service Type for an SSH User

<table>
<thead>
<tr>
<th>Table 632</th>
<th>Specify the service type of an SSH user:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Specify a service type for an SSH user</td>
<td>ssh user username service-type { stelnet</td>
</tr>
</tbody>
</table>

**CAUTION:** If the **ssh user service-type** command is executed with a username
that does not exist, the system will automatically create the SSH user. However,
the user cannot log in unless you specify an authentication type for it.

### Configuring SSH Management

The SSH server provides a number of management functions that prevent illegal
operations such as malicious password guess, to further guarantee the security of
SSH connections.

<table>
<thead>
<tr>
<th>Table 633</th>
<th>Configure SSH management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Command</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>Set SSH authentication timeout time</td>
<td>ssh server timeout seconds</td>
</tr>
<tr>
<td>Set SSH authentication retry times</td>
<td>ssh server authentication-retries times</td>
</tr>
<tr>
<td>Configure a login header</td>
<td>header shell text</td>
</tr>
</tbody>
</table>

**CAUTION:**

- You can configure a login header only when the service type is **stelnet**. For
  configuration of service types, see “Specifying a Service Type for an SSH User”.

- For details of the **header** command, see the corresponding section in Login
  Command.
CHAPTER 71: SSH CONFIGURATION

Configuring the Client Public Key on the Server

This configuration is not necessary if the password authentication mode is configured for SSH users.

With the publickey authentication mode configured for an SSH client, you must configure the client’s RSA or DSA host public key(s) on the server for authentication.

You can manually configure the public key or import it from a public key file. In the former case, you can manually copy the client’s public key to the server. In the latter case, the system automatically converts the format of the public key generated by the client to complete the configuration on the server, but the client’s public key should be transferred from the client to the server beforehand through FTP/TFTP.

Table 634 Configure the client’s public key manually

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter public key view</td>
<td>public-key peer keyname</td>
<td></td>
</tr>
<tr>
<td>Enter public key edit view</td>
<td>public-key-code begin</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a public key for the client</td>
<td>Enter the content of the public key</td>
<td>When you input the key data, spaces are allowed between the characters you input (because the system can remove the spaces automatically); you can also press &lt;Enter&gt; to continue your input at the next line. But the key you input should be a hexadecimal digit string coded in the public key format.</td>
</tr>
<tr>
<td>Return to public key view from public key edit view</td>
<td>public-key-code end</td>
<td>-</td>
</tr>
<tr>
<td>Exit public key view and return to system view</td>
<td>peer-public-key end</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 635 Import the RSA public key from a public key file

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Import the public key from a public key file</td>
<td>public-key peer keyname import sshkey filename</td>
<td>Required</td>
</tr>
</tbody>
</table>

Assigning a Public Key to an SSH User

CAUTION: This configuration task is unnecessary if the SSH user’s authentication mode is password.

For the publickey authentication mode, you must specify the client’s public key on the server for authentication.
Both the keywords **publickey** and **rsa-key** represent the public key, and have the same implementation.

### Specifying a Source IP Address/Interface for the SSH Server

This configuration task allows you to specify a source IP address or interface for the SSH server, which is used by clients as the destination.

#### Table 637  Specify a source IP address/interface for the SSH server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Specify a source IP address for the SSH server</td>
<td><strong>ssh-server source-ip</strong> ip-address</td>
<td>Required By default, the system determines the IP address for clients to access.</td>
</tr>
<tr>
<td>Specify a source interface for the SSH server</td>
<td><strong>ssh-server source-interface</strong> interface-type interface-number</td>
<td>Required By default, the system determines the interface for clients to access.</td>
</tr>
</tbody>
</table>

### Configuring the SSH Client

An SSH client software or SSH2-capable switch can serve as an SSH client to access the SSH server.

#### SSH Client Configuration Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the SSH client</td>
<td>Using an SSH client software Use either approach</td>
</tr>
</tbody>
</table>

#### Configuring the SSH Client Using an SSH Client Software

A variety of SSH client software are available, such as PuTTY and OpenSSH. For an SSH client to establish a connection with an SSH server, use the following commands:

#### Table 639  Configuration tasks for using a client software

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Generate a client key&quot;</td>
<td>Required for <strong>publickey</strong> authentication; unnecessary for <strong>password</strong> authentication</td>
</tr>
<tr>
<td>&quot;Specify the IP address of the Server&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Select a protocol for remote connection&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>
CHAPTER 71: SSH CONFIGURATION

Selecting the protocol for remote connection as SSH. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, and SSH. To establish an SSH connection, you must select SSH.

Selecting the SSH version because the device supports SSH 2.0.

Specifying the private key file. On the server, if public key authentication is enabled for an SSH user and a public key is set for the user, the private key file corresponding to the public key must be specified on the client. RSA key pairs and DSA key pairs are generated by a tool of the client software.

The following uses the PuTTY Version 0.58 client software to illustrate how to configure the SSH client.

**Generate a client key**

To generate a client key, run PuTTYGen.exe, and select from the Parameters area the type of key you want to generate, either SSH-2 RSA or SSH-2 DSA, then click Generate.

![PuTTY Key Generator](image)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Select an SSH version”</td>
<td>Required</td>
</tr>
<tr>
<td>“Open an SSH connection with publickey authentication”</td>
<td>Required for <strong>publickey</strong> authentication; unnecessary for <strong>password</strong> authentication</td>
</tr>
<tr>
<td>“Open an SSH connection with password authentication”</td>
<td>Required for <strong>publickey</strong> authentication; unnecessary for <strong>password</strong> authentication</td>
</tr>
</tbody>
</table>

Figure 245  Generate a client key (1)
Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in Figure 246. Otherwise, the process bar stops moving and the key pair generating process is stopped.

**Figure 246**  Generate the client keys (2)

After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.
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 precaution. Click **Yes** and enter the name of the file for saving the private key (**private** in this case) to save the private key.

To generate RSA public key in PKCS format, run SSHKEY.exe, click **Browse** and select the public key file, and then click **Convert**.
Figure 249  Generate the client keys (5)

Specify the IP address of the Server
Launch PuTTY.exe. The following window appears.
In the **Host Name (or IP address)** text box, enter the IP address of the server. Note that there must be a route available between the IP address of the server and the client.

**Select a protocol for remote connection**

As shown in Figure 250, select **SSH** under **Protocol**.

**Select an SSH version**

From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 251 appears.
Figure 251  SSH client configuration interface 2

Under Protocol options, select 2 from Preferred SSH protocol version.

Some SSH client software, for example, Tectia client software, supports the DES algorithm only when the ssh1 version is selected. The PuTTY client software supports DES algorithm negotiation ssh2.

Open an SSH connection with password authentication

From the window shown in Figure 251, click Open. If the connection is normal, you will be prompted to enter the username and password.

Enter the username and password to establish an SSH connection.

To log out, enter the quit command.

Open an SSH connection with publickey authentication

If a user needs to be authenticated with a public key, the corresponding private key file must be specified. A private key file is not required for password-only authentication.

From the category on the left of the window, select Connection/SSH/Auth. The following window appears.
**Figure 252** SSH client configuration interface 3

Click **Browse**… to bring up the file selection window, navigate to the private key file and click **Open**. If the connection is normal, a user will be prompted for a username. Once passing the authentication, the user can log onto the server.

### Configuring the SSH Client on an SSH2-Capable Switch

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configure whether first-time authentication is supported”</td>
<td>Optional</td>
</tr>
<tr>
<td>Establish the connection between the SSH client and server</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Configure 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 enabled**, an SSH client that is not configured with the server host public key can continue accessing the server when it accesses the server for the first time, and it will save the host public key on the client for use in subsequent authentications.

- **With first-time authentication disabled**, an SSH client that is not configured with the server host public key will be denied access to 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.
Establish the connection between the SSH client and server

The client’s method of establishing an SSH connection to the SSH server varies with authentication types. See Table 643 for details.

**Table 643** Establish an SSH connection

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>Required</td>
</tr>
<tr>
<td>Start the client to establish a</td>
<td>`ssh2 { host-ip</td>
<td>host-name } { port-num } [ identity-key { dsa</td>
</tr>
<tr>
<td>connection with an SSH server</td>
<td></td>
<td>In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client. HMAC: Hash-based message authentication code Note that: The <code>identity-key</code> keyword is unnecessary in password authentication and optional in public key authentication.</td>
</tr>
</tbody>
</table>

When logging into the SSH server using public key authentication, an SSH client needs to read the local private key for authentication. As two algorithms (RSA or DSA) are available, the `identity-key` keyword must be used to specify one algorithm in order to get the correct private key.
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.

Table 644 Specify a source IP address/interface for the SSH client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Specify a source IP address</td>
<td>ssh2 source-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td>for the SSH client.</td>
<td></td>
<td>By default, the system determines a source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>address.</td>
</tr>
<tr>
<td>Specify a source interface</td>
<td>ssh2 source-interface</td>
<td>Required</td>
</tr>
<tr>
<td>for the SSH client.</td>
<td>interface-type</td>
<td>By default, the system determines a source</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>interface.</td>
</tr>
</tbody>
</table>

Displaying and Maintaining SSH Configuration

After completing the above configuration, you can execute the `display` command in any view to display the configuration information and running status of SSH, so as to verify your configuration.

Table 645 Display SSH configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display local public key(s)</td>
<td>display public-key local {</td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
<tr>
<td></td>
<td>dsa</td>
<td>rsa } public</td>
</tr>
<tr>
<td>Display information about</td>
<td>display public-key peer [</td>
<td></td>
</tr>
<tr>
<td>public key(s)</td>
<td>brief</td>
<td>name pubkey-name ]</td>
</tr>
<tr>
<td>Display SSH status and session</td>
<td>display ssh server { session</td>
<td>status }</td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display SSH user information</td>
<td>display ssh user-information [ username</td>
<td></td>
</tr>
<tr>
<td></td>
<td>]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display ssh-server source-ip</td>
<td></td>
</tr>
<tr>
<td>Display the current source IP address</td>
<td>display ssh2 source-ip</td>
<td></td>
</tr>
<tr>
<td>or the IP address of the source interface specified for the SSH server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display the current source IP address</td>
<td>display ssh server-info</td>
<td></td>
</tr>
<tr>
<td>specified for the SSH Client.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display the mappings between host public keys and SSH servers saved on a client</td>
<td>display ssh server-info</td>
<td></td>
</tr>
</tbody>
</table>

Commands with the Same Functions

Now that DSA asymmetric key algorithm is supported, some of the SSH configuration commands have changed. To be compatible with the original SSH configuration, the original commands of those changed are still supported. These commands are listed in Table 646.

Table 646 List of SSH configuration commands with the same functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Original commands</th>
<th>Current commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display local RSA public key(s)</td>
<td>display rsa local-key-pair public</td>
<td>display public-key local rsa public</td>
</tr>
</tbody>
</table>
SSH Configuration Examples

When the Switch Acts as the SSH Server and the Authentication Type is Password

Network requirements
As shown in Figure 253, establish an SSH connection between the host (SSH Client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Password authentication is required.

Network diagram

**Figure 253**  Network diagram of SSH server configuration using password authentication

- [Network diagram]

Configuration procedure

- Configure the SSH server
  
  ```
  # Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.
  ```
Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

# Generate RSA and DSA key pairs.
[5500] public-key local create rsa
[5500] public-key local create dsa

# Set the authentication mode for the user interfaces to AAA.
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme

# Enable the user interfaces to support SSH.
[5500-ui-vty0-4] protocol inbound ssh

# Create local client client001, and set the authentication password to abc, protocol type to SSH, and command privilege level to 3 for the client.
[5500] local-user client001
[5500-luser-client001] password simple abc
[5500-luser-client001] service-type ssh level 3

# Specify the authentication method of user client001 as password.
[5500] ssh user client001 authentication-type password

- Configure the SSH client

  # Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.
  # Configure the SSH client software to establish a connection to the SSH server.
Take SSH client software **Putty** (version 0.58) as an example:

1. Run PuTTY.exe to enter the following configuration interface.

**Figure 254**  SSH client configuration interface

![PuTTY Configuration Interface](image)

In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

2. From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 255 appears.
CHAPTER 71: SSH CONFIGURATION

Figure 255  SSH client configuration interface 2

3  Under Protocol options, select 2 from Preferred SSH protocol version.

4  Click Open. If the connection is normal, you are prompted to enter the user name client001 and password abc. Once authentication succeeds, you will log onto the server.

When the Switch Acts as an SSH Server and the Authentication Type is Publickey

Network requirements
As shown in Figure 256, establish an SSH connection between the host (SSH client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Publickey authentication is required.

Network diagram

Figure 256  Network diagram of SSH server configuration

Configuration procedure

Under the publickey authentication mode, either the RSA or DSA public key can be generated for the server to authenticate the client. Here takes the RSA public key as an example.

- Configure the SSH server
# Create a VLAN interface on the switch and assign an IP address, which the
SSH client will use as the destination for SSH connection.

```plaintext
<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[5500-Vlan-interface1] quit
```

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

# Generate RSA and DSA key pairs.

```plaintext
[5500] public-key local create rsa
[5500] public-key local create dsa
```

# Set the authentication mode for the user interfaces to AAA.

```plaintext
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```plaintext
[5500-ui-vty0-4] protocol inbound ssh
```

# Set the client's command privilege level to 3

```plaintext
[5500-ui-vty0-4] user privilege level 3
[5500-ui-vty0-4] quit
```

# Configure the authentication type of the SSH client named client 001 as publickey.

```plaintext
[5500] ssh user client001 authentication-type publickey
```

Before performing the following steps, you must generate an RSA public key pair (using the client software) on the client, save the key pair in a file named public, and then upload the file to the SSH server through FTP or TFTP. For details, refer to “Configuring the SSH Client” on page 841.

# Import the client’s public key named Switch001 from file public.

```plaintext
[5500] public-key peer Switch001 import sshkey public
```

# Assign the public key Switch001 to client client001.

```plaintext
[5500] ssh user client001 assign publickey Switch001
```

- Configure the SSH client
# Generate an RSA key pair, using PuTTY version 0.58 as an example.

1. Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

**Figure 257** 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 258. Otherwise, the process bar stops moving and the key pair generating process is stopped.
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (public in this case).
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 private key (*private.ppk* in this case).

**Figure 260** Generate a client key pair (4)

After a public key pair is generated, you need to upload the public key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

# Establish a connection with the SSH server

1. Launch PuTTY.exe to enter the following interface.

   **Figure 261** SSH client configuration interface 1

   In the **Host Name (or IP address)** text box, enter the IP address of the server.

   2. From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 262 appears.
Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

3 Select **Connection/SSH/Auth**. The following window appears.
4 Click **Browse...** to bring up the file selection window, navigate to the private key file and click **OK**.

5 Click **Open**. If the connection is normal, you are prompted to enter the username and password.

6 Specify the requested information and click **OK**.

When the Switch Acts as an SSH Client and the Authentication Type is Password

**Network requirements**

As shown in Figure 264, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name for login is client001 and the SSH server’s IP address is 10.165.87.136. Password authentication is required.

**Network diagram**

**Figure 264** Network diagram of SSH client configuration when using password authentication

**Configuration procedure**

- Configure Switch B
# Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```plaintext
<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[5500-Vlan-interface1] quit
```

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

# Generate RSA and DSA key pairs.

```plaintext
[5500] public-key local create rsa
[5500] public-key local create dsa
```

# Set the authentication mode for the user interfaces to AAA.

```plaintext
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```plaintext
[5500-ui-vty0-4] protocol inbound ssh
[5500-ui-vty0-4] quit
```

# Create local user **client001**, and set the authentication password to abc, the login protocol to SSH, and user command privilege level to 3.

```plaintext
[5500] local-user client001
[5500-luser-client001] password simple abc
[5500-luser-client001] service-type ssh level 3
[5500-luser-client001] quit
```

# Configure the authentication type of user client001 as password.

```plaintext
[5500] ssh user client001 authentication-type password
```

**Configure Switch A**

# Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client’s address in an SSH connection.

```plaintext
<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[5500-Vlan-interface1] quit
```

# Establish a connection to the server 10.165.87.136.

```plaintext
[5500] 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. Do you continue to access it?(Y/N):y

Do you want to save the server’s public key?(Y/N):n

Enter password:

```
******************************************************************************
* Copyright(c) 2004-2007 3Com Corporation                                  *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-switch fabricering shall be allowed.         *
******************************************************************************
```
**Network requirements**

As shown in Figure 265, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server’s IP address is 10.165.87.136. Publickey authentication is required.

**Network diagram**

**Figure 265** Network diagram of SSH client configuration when using publickey authentication

![Network diagram](Network-diagram.png)

**Configuration procedure**

In public key authentication, you can use either RSA or DSA public key. Here takes the DSA public key as an example.

- Configure Switch B

  ```
  # Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

  <5500> system-view
  [5500] interface vlan-interface 1
  [5500-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
  [5500-Vlan-interface1] quit

  # Generate RSA and DSA key pairs.
  [5500] public-key local create rsa
  [5500] public-key local create dsa

  # Set the authentication mode for the user interfaces to AAA.
  [5500] user-interface vty 0 4
  [5500-ui-vty0-4] authentication-mode scheme

  # Enable the user interfaces to support SSH.
  [5500-ui-vty0-4] protocol inbound ssh

  # Set the user command privilege level to 3.
  [5500-ui-vty0-4] user privilege level 3
  [5500-ui-vty0-4] quit

  # Specify the authentication type of user client001 as publickey.
  [5500] ssh user client001 authentication-type publickey
  ```

Before doing the following steps, you must first generate a DSA public key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to Configure Switch A below.

- Import the client public key pair named Switch001 from the file Switch001.

  ```
  [5500] public-key peer Switch001 import sshkey Switch001
  ```

- Assign the public key Switch001 to user client001.

  ```
  [5500] user client001 sshkey Switch001
  ```
SSH Configuration Examples

[5500] ssh user client001 assign publickey Switch001

- Configure Switch A
  
  # Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

  ```
  <5500> system-view
  [5500] interface vlan-interface 1
  [5500-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
  [5500-Vlan-interface1] quit
  # Generate a DSA key pair
  [5500] public-key local create dsa
  # Export the generated DSA key pair to a file named Switch001.
  [5500] public-key local export dsa ssh2 Switch001
  ```

  After the key pair is generated, you need to upload the public key file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

  ```
  # Establish an SSH connection to the server 10.165.87.136.
  [5500] ssh2 10.165.87.136 identity-key dsa
  Username: client001
  Trying 10.165.87.136 ... Press CTRL+K to abort
  Connected to 10.165.87.136 ...

  The Server is not authenticated. Do you continue to access it?(Y/N):y
  Do you want to save the server’s public key?(Y/N):n
  *************************************************************************
  * Copyright(c) 2004-2007 3Com Corporation..                        *
  * Without the owner’s prior written consent,                      *
  * no decompiling or reverse-switch fabricering shall be allowed.  *
  *************************************************************************
  ```

- Network requirements
  
  As shown in Figure 266, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server’s IP address is 10.165.87.136. The **publickey** authentication mode is used to enhance security.

- Network diagram
  
  **Figure 266**  Network diagram of SSH client configuration

- Configuration procedure
  
  - Configure Switch B

When the Switch Acts as an SSH Client and First-time authentication is not Supported
CHAPTER 71: SSH CONFIGURATION

# Create a VLAN interface on the switch and assign an IP address for it to serve as the destination of the client.

```shell
<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[5500-Vlan-interface1] quit
```

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

# Generate RSA and DSA key pairs.

```shell
[5500] public-key local create rsa
[5500] public-key local create dsa
```

# Set AAA authentication on user interfaces.

```shell
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme
```

# Configure the user interfaces to support SSH.

```shell
[5500-ui-vty0-4] protocol inbound ssh
```

# Set the user command privilege level to 3.

```shell
[5500-ui-vty0-4] user privilege level 3
[5500-ui-vty0-4] quit
```

# Specify the authentication type for user client001 as publickey.

```shell
[5500] ssh user client001 authentication-type publickey
```

Before doing the following steps, you must first generate a DSA key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the following Configure Switch A.

# Import the client's public key file Switch001 and name the public key as Switch001.

```shell
[5500] public-key peer Switch001 import sshkey Switch001
```

# Assign public key Switch001 to user client001

```shell
[5500] ssh user client001 assign publickey Switch001
```

# Export the generated DSA host public key pair to a file named Switch002.

```shell
[5500] public-key local export dsa ssh2 Switch002
```

When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP.

Configure Switch A

# Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```shell
<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[5500-Vlan-interface1] quit
```
# Generate a DSA key pair

[5500] public-key local create dsa

# Export the generated DSA key pair to a file named Switch001.

[5500] public-key local export dsa ssh2 Switch001

After generating the key pair, you need to upload the key pair file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

# Disable first-time authentication on the device.

[5500] undo ssh client first-time

When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP. For details, refer to the above section Configure Switch B.

# Import the public key pair named Switch002 from the file Switch002.

[5500] public-key peer Switch002 import sshkey Switch002

# Specify the host public key pair name of the server.

[5500] ssh client 10.165.87.136 assign publickey Switch002

# Establish the SSH connection to server 10.165.87.136.

[5500] ssh2 10.165.87.136 identity-key dsa
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...
*************************************************************************
* Copyright(c) 2004-2007 3Com Corporation                              *
* Without the owner’s prior written consent,                          *
* no decompiling or reverse-switch fabricering shall be allowed.      *
*************************************************************************
File System Management Configuration

Introduction to File System

To facilitate management on the switch's memory, the Switch 5500 provides the file system function, allowing you to access and manage the files and directories. You can create, remove, copy or delete a file through command lines, and you can manage files using directories.

File System Configuration Tasks

The Switch 5500 supports intelligent resilient framework (IRF), and allows you to input a file path and file name in one of the following ways:

- In URL (universal resource locator) format and starting with `unit[No.]>flash:/` (where `[No.]` represents the unit ID of a switch). This method is used to specify a file on a specified unit. For example, if the unit ID of a switch is 1, the URL of a file named `text.txt` and residing in the root directory must be `unit1>flash:/text.txt`.
- In URL format and starting with `flash:/`. This method can be used to specify a file in the Flash memory of the current unit.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory.

Directory Operations

The file system provides directory-related functions, such as:

- Creating/deleting a directory
- Displaying the current work directory, or contents in a specified directory

Table 647 describes the directory-related operations.

<table>
<thead>
<tr>
<th>Configuration task</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory operation</td>
<td>Optional</td>
<td>&quot;Directory Operations&quot;</td>
</tr>
<tr>
<td>File operation</td>
<td>Optional</td>
<td>&quot;File Operations&quot;</td>
</tr>
<tr>
<td>Flash memory operation</td>
<td>Optional</td>
<td>&quot;Flash Memory Operations&quot;</td>
</tr>
<tr>
<td>Prompt mode configuration</td>
<td>Optional</td>
<td>&quot;Prompt Mode Configuration&quot;</td>
</tr>
</tbody>
</table>

Perform the following configuration in user view.

Table 648  Directory operations

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a directory</td>
<td>mkdir directory</td>
<td>Optional</td>
</tr>
<tr>
<td>Delete a directory</td>
<td>rmdir directory</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the current work directory</td>
<td>pwd</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the information about specific directories and files</td>
<td>dir [/all] [/fabric] [file-url]</td>
<td>Optional</td>
</tr>
<tr>
<td>Enter a specified directory</td>
<td>cd directory</td>
<td>Optional</td>
</tr>
</tbody>
</table>

- Only empty directories can be deleted by using the rmdir command.
- In the output information of the dir /all command, deleted files (that is, those stored in the recycle bin) are embraced in brackets.

File Operations  The file system also provides file-related functions listed in Table 649.

Perform the following configuration in user view. Note that the execute command should be executed in system view.

Table 649  File operations

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a file</td>
<td>delete [/unreserved] [file-url]</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>delete {running-files</td>
<td>standby-files} [/fabric] [/unreserved]</td>
</tr>
<tr>
<td>Restore a file in the recycle bin</td>
<td>undelete file-url</td>
<td>Optional</td>
</tr>
<tr>
<td>Delete a file from the recycle bin</td>
<td>reset recycle-bin</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>[file-url] [/force]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reset recycle-bin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[/fabric]</td>
<td></td>
</tr>
<tr>
<td>Upgrade the software of the whole fabric</td>
<td>update fabric file-name</td>
<td>Optional</td>
</tr>
<tr>
<td>Rename a file</td>
<td>rename fileurl-source fileurl-dest</td>
<td>Optional</td>
</tr>
<tr>
<td>Copy a file</td>
<td>copy fileurl-source fileurl-dest</td>
<td>Optional</td>
</tr>
<tr>
<td>Move a file</td>
<td>move fileurl-source fileurl-dest</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the content of a file</td>
<td>more file-url</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the information about a directory or a file</td>
<td>dir [/all] [/fabric] [file-url]</td>
<td>Optional</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Execute the specified batch file</td>
<td>execute filename</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Available in system view.</td>
<td></td>
</tr>
</tbody>
</table>
CAUTION:
- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the `delete` command without the `/unreserved` keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the `reset recycle-bin` command.
- Use the `update fabric` command after all traffic flows are stopped.
- The `dir /all` command displays the files in the recycle bin in square brackets.
- If the configuration files are deleted, the switch adopts the null configuration when it starts up next time.

Flash Memory Operations
In user view, perform the following Flash memory operations using the commands listed in Table 650.

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format the Flash memory</td>
<td><code>format device</code></td>
<td>Required</td>
</tr>
<tr>
<td>Restore space on the Flash memory</td>
<td><code>fixdisk device</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

CAUTION: The `format` operation leads to the loss of all files, including the configuration files, on the Flash memory and is irretrievable.

Prompt Mode Configuration
You can set the prompt mode of the current file system to `alert` or `quiet`. In alert mode, the file system will give a prompt for confirmation if you execute a command which may cause data loss, for example, deleting or overwriting a file. In quiet mode, such prompt will not be displayed.

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
</tbody>
</table>
| Configure the prompt mode of the file system | `file prompt { alert | quiet }` | Required By default, the prompt mode of the file system is `alert`.

File System Configuration Example
# Display all the files in the root directory of the file system on the local unit.

```
<5500> dir /all
Directory of unit1>flash:/

1 (*) -rw- 5822215 Jan 01 1970 00:07:03 test.bin
2 -rwh 4 Apr 01 2000 23:55:49 snmpboots
3 -rwh 428 Apr 02 2000 00:47:30 hostkey
4 -rwh 572 Apr 02 2000 00:47:38 serverkey
5 -rw- 1220 Apr 02 2000 00:06:57 song.cfg
6 -rw- 5026103 Jan 01 1970 00:04:34 testv1r1.bin
7 -rw- 88 Apr 01 2000 23:55:53 private-data.txt
8 (*) -rw- 1376 Apr 02 2000 01:56:28 config.cfg

15367 KB total (4634 KB free)
```
# Copy the file flash:/config.cfg to flash:/test/, with 1.cfg as the name of the new file.

\[5500\] copy flash:/config.cfg flash:/test/1.cfg
Copy unit1>flash:/config.cfg to unit1>flash:/test/1.cfg? [Y/N]: y
...
%Copy file unit1>flash:/config.cfg to unit1>flash:/test/1.cfg...Done.

# Display the file information after the copy operation.

\[5500\] dir /all
Directory of unit1>flash: /

1 (*) -rw- 5822215 Jan 01 1970 00:07:03 test.bin
2 -rwh 4 Apr 01 2000 23:55:49 snmpboots
3 -rwh 428 Apr 02 2000 00:47:30 hostkey
4 -rwh 572 Apr 02 2000 00:47:38 serverkey
5 -rw- 1220 Apr 02 2000 00:06:57 song.cfg
6 -rw- 5026103 Jan 01 1970 00:04:34 testv1r1.bin
7 -rwh 88 Apr 01 2000 23:55:53 private-data.txt
8 (*) -rw- 1376 Apr 04 2000 01:56:28 config.cfg
9 drw- - Apr 04 2000 04:50:07 test

15367 KB total (4631 KB free)

(*) -with main attribute  (b) -with backup attribute
(*b) -with both main and backup attribute

\[5500\] dir unit1>flash:/test/
Directory of unit1>flash:/test/

1 -rw- 1376 Apr 02 2000 04:50:30 1.cfg

15367 KB total (2025 KB free)

(*) -with main attribute  (b) -with backup attribute
(*b) -with both main and backup attribute

---

**File Attribute Configuration**

**Introduction to File Attributes**

The following three startup files support file attribute configuration:

- **App files**: An app file is an executable file, with .bin as the extension.
- **Configuration files**: A configuration file is used to store and restore configuration, with .cfg as the extension.
- **Web files**: A Web file is used for Web-based network management, with .web as the extension.

The app files, configuration files, and Web files support three kinds of attributes: main, backup and none, as described in Table 652.
A file can have both the main and backup attributes. Files of this kind are labeled *b.

Note that, there can be only one app file, one configuration file and one Web file with the main attribute in the Flash memory. If a newly created file is configured to be with the main attribute, the existing file with the main attribute in the Flash memory will lose its main attribute. This circumstance also applies to the file with the backup attribute in the Flash memory.

File operations and file attribute operations are independent. For example, if you delete a file with the main attribute from the Flash memory, the other files in the flash memory will not possess the main attribute. If you download a valid file with the same name as the deleted file to the flash memory, the file will possess the main attribute.

After the switch's Boot ROM is upgraded, the original default application file has the main attribute.

### Booting with the Startup File

The device selects the main startup file as the preferred startup file. If the device fails to boot with the main startup file, it boots with the backup startup file.

For the Web file and configuration file, 3Com may provide a corresponding default file when releasing software versions. When booting, the device selects the startup files in a specific order. The device selects Web files in the following order:

1. If the default Web file exists, the device will boot with the default Web file;
2. If the default Web file does not exist, but the main Web file exists, the device will boot with the main Web file;
3. If neither the default Web file nor the main Web file exists, but the backup Web file exists, the device will boot with the backup Web file;
4. If neither of the default Web file, main Web file and backup Web exists, the device considers that no Web file exists.

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Feature</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>Identifies main startup files. The main startup file is preferred for a switch to start up.</td>
<td>In the Flash memory, there can be only one app file, one configuration file and one Web file with the main attribute.</td>
<td>(*)</td>
</tr>
<tr>
<td>backup</td>
<td>Identifies backup startup files. The backup startup file is used after a switch fails to start up using the main startup file.</td>
<td>In the Flash memory, there can be only one app file, one configuration file and one Web file with the backup attribute.</td>
<td>(b)</td>
</tr>
<tr>
<td>none</td>
<td>Identifies files that are neither of main attribute nor backup attribute.</td>
<td>-</td>
<td>None</td>
</tr>
</tbody>
</table>

### Table 652  Descriptions on file attributes
For instructions on selecting the configuration file when the device boots, refer to “Configuration File Management” on page 87.

**Configuring File Attributes**

You can configure and view the main attribute or backup attribute of the file used for the next switch restart, as well as change the main or backup attribute of the file.

Perform the configuration steps in Table 653 in user view. The `display` commands can be executed in any view.

**Table 653 Configure file attributes**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the app file with the main attribute for the next startup</td>
<td><code>boot boot-loader file-url [fabric ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the app file with the backup attribute for the next startup</td>
<td><code>boot boot-loader backup-attribute file-url [fabric ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the Web file and its attribute</td>
<td>`boot web-package webfile {backup</td>
<td>main }`</td>
</tr>
<tr>
<td>Switch the file attributes between main and backup</td>
<td>`boot attribute-switch { all</td>
<td>app</td>
</tr>
<tr>
<td>Specify to enable user to use the customized password to enter the BOOT menu</td>
<td><code>startup bootrom-access enable</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Display the information about the app file used as the startup file</td>
<td><code>display boot-loader [ unit unit-id ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Display information about the Web file used by the device</td>
<td><code>display web package</code></td>
<td>Available in any view</td>
</tr>
</tbody>
</table>

**CAUTION:**

- Before configuring the main or backup attribute for a file in the fabric, make sure the file already exists on all devices in the fabric.
- The configuration of the main or backup attribute of a Web file takes effect immediately without restarting the switch.
- After upgrading a Web file, you need to specify the new Web file in the Boot menu after restarting the switch or specify a new Web file by using the `boot web-package` command. Otherwise, Web server cannot function normally.
- Currently, a configuration file has the extension of cfg and resides in the root directory of the Flash memory.
- For the detailed configuration of configuration file attributes, refer to “Configuration File Management” on page 87.
Introduced to Configuration File Backup and Restoration

Formerly, you can only back up and restore the configuration file of the units one by one in a fabric system.

By using the configuration file backup and restoration feature, you can easily back up and restore the configuration files in the whole fabric as well as in a specific unit.

In the backup process, the system first saves the current configuration of a unit to the startup configuration file, and then uploads the file to the TFTP server. In the restore process, the system downloads the startup configuration file from the TFTP server to the local unit.

The configurations of different units in the fabric system can be saved in different .cfg configuration files on the TFTP server. These configuration files form the startup configuration of the whole fabric.

File Backup and Restoration

Configuration prerequisites

Before performing the following operations, you must first ensure that:

- The relevant units support TFTP client.
- The TFTP server is started
- A route exists between the TFTP server and TFTP client.

Configuration procedure

Perform the following operations in user view.

Table 654 Back up and restore configuration file

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the current configuration of a specified unit</td>
<td>backup unit unit-id current-configuration to { dest-addr</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>dest-hostname } filename.cfg</td>
<td></td>
</tr>
<tr>
<td>Back up the current configuration of the whole fabric system</td>
<td>backup fabric current-configuration to { dest-addr</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>dest-hostname } filename.cfg</td>
<td></td>
</tr>
<tr>
<td>Restore the startup configuration of a specified unit</td>
<td>restore unit unit-id startup-configuration from { source-addr</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>source-hostname } filename.cfg</td>
<td></td>
</tr>
<tr>
<td>Restore the startup configuration of the whole fabric system</td>
<td>restore fabric startup-configuration from { source-addr</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>source-hostname } filename.cfg</td>
<td></td>
</tr>
</tbody>
</table>
**FTP AND SFTP CONFIGURATION**

### Introduction to FTP

**FTP** (file transfer protocol) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local client. FTP uses TCP ports 20 and 21 for data transfer and control command transfer respectively. Basic FTP operations are described in RFC 959.

FTP-based file transmission is performed in the following two modes:

- Binary mode for program file transfer
- ASCII mode for text file transfer

A 3Com Switch 5500 can operate as an FTP client or the FTP server in FTP-employed data transmission:

**Table 655** The Switch 5500 FTP Roles

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP server</td>
<td>An Ethernet switch can operate as an FTP server to provide file transmission services for FTP clients. You can log in to a switch operating as an FTP server by running an FTP client program on your PC to access files on the FTP server.</td>
<td>The prerequisite is that a route exists between the switch and the PC.</td>
</tr>
<tr>
<td>FTP client</td>
<td>In this case, you need to establish a connection between your PC and the switch through a terminal emulation program or Telnet, execute the <code>ftp X.X.X.X</code> command on your PC. (X.X.X.X is the IP address of an FTP server or a host name), and enter your user name and password in turn. A switch can operate as an FTP client, through which you can access files on the FTP server.</td>
<td></td>
</tr>
</tbody>
</table>
With the Switch 5500 operating as an FTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise when an FTP client is uploading files to the FTP server (the Switch 5500), and stops rotating when the file uploading is finished, as shown in Figure 267.

With the Switch 5500 operating as an FTP client, the seven-segment digital LED on the front panel of the switch rotates clockwise when the FTP client (the Switch 5500) is downloading files from an FTP server, and stops rotating when the file downloading is finished, as shown in Figure 267.

Figure 267  Clockwise rotating of the seven-segment digital LED

Introduction to SFTP

Secure FTP (SFTP) is established based on an SSH2 connection. It allows a remote user to log in to a switch to manage and transmit files, providing a securer guarantee for data transmission. In addition, since the switch can be used as a client, you can log in to remote devices to transfer files securely.

<table>
<thead>
<tr>
<th>Item</th>
<th>Configuration task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“FTP Configuration: A Switch Operating as an FTP Server”</td>
<td>“Creating an FTP user”</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>“Enabling an FTP server”</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>“Configuring connection idle time”</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>“Specifying the source interface and source IP address for an FTP server”</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>“Disconnecting a specified user”</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>“Configuring the banner for an FTP server”</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>“Displaying FTP server information”</td>
<td>Optional</td>
</tr>
<tr>
<td>“FTP Configuration: A Switch Operating as an FTP Client”</td>
<td>“Basic configurations on an FTP client”</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>“Specifying the source interface and source IP address for an FTP client”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

FTP Configuration: A Switch Operating as an FTP Server

Creating an FTP user

Configure the user name and password for the FTP user and set the service type to FTP. To use FTP services, a user must provide a user name and password for being authenticated by the FTP server. Only users that pass the authentication have access to the FTP server.
Enabling an FTP server

Table 657  Create an FTP user

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Add a local user and enter local user view</td>
<td>local-user user-name</td>
<td>Required by default, no local user is configured.</td>
</tr>
<tr>
<td>Configure a password for the specified user</td>
<td>password (simple</td>
<td>cipher) password</td>
</tr>
<tr>
<td>Configure the service type as FTP</td>
<td>service-type ftp</td>
<td>Required by default, no service is configured.</td>
</tr>
</tbody>
</table>

Table 658  Enable an FTP server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable the FTP server function</td>
<td>ftp server enable</td>
<td>Required disabled by default.</td>
</tr>
</tbody>
</table>

Only one user can access the Switch 5500 at a given time when the latter operates as an FTP server.

Operating as an FTP server, the Switch 5500 cannot receive a file whose size exceeds its storage space. The clients that attempt to upload such a file will be disconnected with the FTP server due to lack of storage space on the FTP server.

When you log in to a Fabric consisting of multiple switches through an FTP client, after the FTP client passes authentication, you can log in to the master device of the Fabric.

To protect unused sockets against attacks, the Switch 5500 provides the following functions:

- TCP 21 is enabled only when you start the FTP server.
- TCP 21 is disabled when you shut down the FTP server.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Table 659  Configure connection idle time

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure the connection idle time for the FTP server</td>
<td>ftp timeout minutes</td>
<td>Optional 30 minutes by default.</td>
</tr>
</tbody>
</table>
Specifying the source interface and source IP address for an FTP server

You can specify the source interface and source IP address for an FTP server to enhance server security. After this configuration, FTP clients can access this server only through the IP address of the specified interface or the specified IP address.

**Source interface** refers to the existing VLAN interface or Loopback interface on the device. **Source IP address** refers to the IP address configured for the interface on the device. Each source interface corresponds to a source IP address. Therefore, specifying a source interface for the FTP server is the same as specifying the IP address of this interface as the source IP address.

| Table 660 Specify the source interface and source IP address for an FTP server |
|---|---|---|
| Operation | Command | Description |
| Enter system view | `system-view` | - |
| Specify the source interface for an FTP server | `ftp-server source-interface interface-type interface-number` | Use either command Not specified by default. |
| Specifying the source IP address for an FTP server | `ftp-server source-ip ip-address` | |

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the `ip-address` argument must be an IP address on the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- You can specify only one source interface or source IP address for the FTP at one time. That is, only one of the commands `ftp-server source-interface` and `ftp-server source-ip` can be valid at one time. If you execute both of them, the new setting will overwrite the original one.
- If the switch (FTP server) is the command switch or member switch in a cluster, do not use the `ftp-server source-ip` command to specify the private IP address of the cluster as the source IP address of the FTP server. Otherwise, FTP does not take effect.

**Disconnecting a specified user**

On the FTP server, you can disconnect a specified user from the FTP server to secure the network.

| Table 661 Disconnect a specified user |
|---|---|---|
| Operation | Command | Description |
| Enter system view | `system-view` | - |
| On the FTP server, disconnect a specified user from the FTP server | `ftp disconnect user-name` | Required |

With the Switch 5500 operating as the FTP server, if a network administrator attempts to disconnect a user that is uploading/downloadig data to/from the FTP server the Switch 5500 will disconnect the user after the data transmission is completed.
Configuring the banner for an FTP server

Displaying a banner: With a banner configured on the FTP server, when you access the FTP server through FTP, the configured banner is displayed on the FTP client. Banner falls into the following two types:

- Login banner: After the connection between an FTP client and an FTP server is established, the FTP server outputs the configured login banner to the FTP client terminal.

  ![Figure 268 Process of displaying a login banner](image)

- Shell banner: After the connection between an FTP client and an FTP server is established and correct user name and password are provided, the FTP server outputs the configured shell banner to the FTP client terminal.

  ![Figure 269 Process of displaying a shell banner](image)

<table>
<thead>
<tr>
<th>Table 662 Configure the banner display for an FTP server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
</tr>
<tr>
<td>Enter system view</td>
</tr>
<tr>
<td>Configure a login banner</td>
</tr>
<tr>
<td>Configure a shell banner</td>
</tr>
</tbody>
</table>

*For details about the header command, refer to “Logging into an Ethernet Switch” on page 31.*
Displaying FTP server information

After completing the above configuration, you can execute the **display** commands in any view to display the running status of the FTP server and verify your configurations.

**Table 663** Display FTP server information

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about FTP server configurations on a switch</td>
<td><code>display ftp-server</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the source IP address set for an FTP server</td>
<td><code>display ftp-server source-ip</code></td>
<td></td>
</tr>
<tr>
<td>Display the login FTP client on an FTP server</td>
<td><code>display ftp-user</code></td>
<td></td>
</tr>
</tbody>
</table>

**FTP Configuration: A Switch Operating as an FTP Client**

**Basic configurations on an FTP client**

By default a switch can operate as an FTP client. In this case you can connect the switch to the FTP server to perform FTP-related operations (such as creating/removing a directory) by executing commands on the switch. Table 664 lists the operations that can be performed on an FTP client.

**Table 664** Basic configurations on an FTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter FTP client view</td>
<td>`ftp [ cluster</td>
<td>remote-server [ port-number ] ]`</td>
</tr>
<tr>
<td>Specify to transfer files in ASCII characters</td>
<td><code>ascii</code></td>
<td>Use either command</td>
</tr>
<tr>
<td>Specify to transfer files in binary streams</td>
<td><code>binary</code></td>
<td>By default, files are transferred in ASCII characters.</td>
</tr>
<tr>
<td>Set the data transfer mode to passive</td>
<td><code>passive</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Change the working directory on the remote FTP server</td>
<td><code>cd pathname</code></td>
<td><code>passive</code> by default.</td>
</tr>
<tr>
<td>Change the working directory to be the parent directory</td>
<td><code>cdup</code></td>
<td></td>
</tr>
<tr>
<td>Get the local working path on the FTP client</td>
<td><code>lcd</code></td>
<td></td>
</tr>
<tr>
<td>Display the working directory on the FTP server</td>
<td><code>pwd</code></td>
<td></td>
</tr>
<tr>
<td>Create a directory on the remote FTP server</td>
<td><code>mkdir pathname</code></td>
<td></td>
</tr>
<tr>
<td>Remove a directory on the remote FTP server</td>
<td><code>rmdir pathname</code></td>
<td></td>
</tr>
<tr>
<td>Delete a specified file</td>
<td><code>delete remotefile</code></td>
<td></td>
</tr>
</tbody>
</table>
Table 664  Basic configurations on an FTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query a specified file on the FTP server</td>
<td>dir (remotefile</td>
<td>localfile)</td>
</tr>
<tr>
<td></td>
<td>ls (remotefile</td>
<td>localfile)</td>
</tr>
<tr>
<td></td>
<td>get remotefile</td>
<td>localfile</td>
</tr>
<tr>
<td>Download a remote file from the FTP server</td>
<td>put localfile</td>
<td>remotefile</td>
</tr>
<tr>
<td>Upload a local file to the remote FTP server</td>
<td>rename remote-source</td>
<td>remote-dest</td>
</tr>
<tr>
<td>Rename a file on the remote server</td>
<td>user username</td>
<td>password</td>
</tr>
<tr>
<td>Log in with the specified user name and password</td>
<td>open (ip-address</td>
<td>server-name</td>
</tr>
<tr>
<td>Connect to a remote FTP server</td>
<td>disconnect</td>
<td>close</td>
</tr>
<tr>
<td>Terminate the current FTP connection without exiting FTP client view</td>
<td>quit</td>
<td>bye</td>
</tr>
<tr>
<td>Terminate the current FTP connection and return to user view</td>
<td>remotehelp (protocol-command)</td>
<td></td>
</tr>
<tr>
<td>Display the online help about a specified command concerning FTP</td>
<td>verbose</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Specifying the source interface and source IP address for an FTP client
You can specify the source interface and source IP address for a switch acting as an FTP client, so that it can connect to a remote FTP server.

Table 665  Specify the source interface and source IP address for an FTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the source interface used for the current connection</td>
<td>ftp (cluster</td>
<td>remote-server</td>
</tr>
<tr>
<td></td>
<td>source-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td>Specify the source IP address used for the current connection</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
CHAPTER 73: FTP AND SFTP CONFIGURATION

■ The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.

■ The value of the ip-address argument must be the IP address of the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.

■ The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between an FTP client and an FTP server, if you specify the source interface/source IP address used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.

■ Only one fixed source interface or source IP address can be set for the FTP client at one time. That is, only one of the commands ftp source-interface and ftp source-ip can be valid at one time. If you execute both of them, the new setting will overwrite the original one.

| Table 665 Specify the source interface and source IP address for an FTP client |
|-----------------------------|-----------------|-----------------|
| Operation | Command | Description |
| Specify an interface as the source interface the FTP client uses every time it connects to an FTP server | ftp source-interface interface-type interface-number | Use either command Not specified by default |
| Specify an IP address as the source IP address the FTP client uses every time it connects to an FTP server | ftp source-ip ip-address |
| Display the source IP address used by an FTP client every time it connects to an FTP server | display ftp source-ip | Available in any view |

Configuration Example: A Switch Operating as an FTP Server

Network requirements
A switch operates as an FTP server and a remote PC as an FTP client. The application switch.bin of the switch is stored on the PC. Upload the application to the remote switch through FTP and use the boot boot-loader command to specify switch.bin as the application for next startup. Reboot the switch to upgrade the switch application and download the configuration file config.cfg from the switch, thus to back up the configuration file.

■ Create a user account on the FTP server with the user name switch and password hello.

■ The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.
Network diagram

Figure 270  Network diagram for FTP configurations: a switch operating as an FTP server

Configuration procedure

1  Configure Switch A (the FTP server)

   # Log in to the switch and enable the FTP server function on the switch. Configure the user name and password used to access FTP services, and specify the service type as FTP (You can log in to a switch through the Console port or by telnetting the switch. See the Login module for detailed information.)

   # Configure the FTP user name as switch, the password as hello, and the service type as FTP.

   <5500>
   <5500> system-view
   [5500] ftp server enable
   [5500] local-user switch
   [5500-luser-switch] password simple hello
   [5500-luser-switch] service-type ftp

2  Configure the PC (FTP client)

   Run an FTP client application on the PC to connect to the FTP server. Upload the application named switch.bin to the root directory of the Flash memory of the FTP server, and download the configuration file named config.cfg from the FTP server. The following takes the command line window tool provided by Windows as an example:

   # Enter the command line window and switch to the directory where the file switch.bin is located. In this example it is in the root directory of C:

   C:\>

   # Access the Ethernet switch through FTP. Input the user name switch and password hello to log in and enter FTP view.

   C:\> ftp 1.1.1.1
   Connected to 1.1.1.1.
   220 FTP service ready.
   User (1.1.1.1:(none)): switch
   331 Password required for switch.
   Password:
   230 User logged in.
   ftp>

   # Upload the switch.bin file.

   ftp> put switch.bin
   200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.
ftp: 75980 bytes received in 5.55 seconds 13.70Kbytes/sec.

# Download the config.cfg file.

ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 3980 bytes received in 8.277 seconds 0.48Kbytes/sec.

This example uses the command line window tool provided by Windows. Follow the instructions in the appropriate section for logging into other FTP clients.

CAUTION:
- If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.
- 3Com series switch is not shipped with FTP client application software. You need to purchase and install it by yourself.

3 Configure Switch A (FTP server)

# After uploading the application, use the boot boot-loader command to specify the uploaded file (switch.bin) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

<5500> boot boot-loader switch.bin
<5500> reboot

For information about the boot boot-loader command and how to specify the startup file for a switch, refer to the “Basic System Configuration and Debugging” on page 929.

FTP Banner Display Configuration Example

Network requirements
Configure the Ethernet switch as an FTP server and the remote PC as an FTP client. After a connection between the FTP client and the FTP server is established and login succeeds, the banner is displayed on the FTP client.

- An FTP user named switch and the password hello have been configured on the FTP server.
- The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.
- Configure the login banner of the switch as login banner appears and the shell banner as shell banner appears.
Network diagram

Figure 271  Network diagram for FTP banner display configuration

Configuration procedure

1  Configure the switch (FTP server)

# Configure the login banner of the switch as login banner appears and the shell banner as shell banner appears. For detailed configuration of other network requirements, see “Configuration Example: A Switch Operating as an FTP Server” on page 882.

```
<5500> system-view
[5500] header login %login banner appears%
[5500] header shell %shell banner appears%
```

2  Configure the PC (FTP client)

# Access the Ethernet switch through FTP. Enter the user name switch and the password hello to log in to the switch, and then enter FTP view. Login banner appears after FTP connection is established. Shell banner appears after the user passes the authentication.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220-login banner appears
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230-shell banner appears
230 User logged in.
ftp>
```

Network requirements

A switch operates as an FTP client and a remote PC as an FTP server. The switch application named switch.bin is stored on the PC. Download it to the switch through FTP and use the boot boot-loader command to specify switch.bin as the application for next startup. Reboot the switch to upgrade the switch application, and then upload the switch configuration file named config.cfg to the switch directory of the PC to back up the configuration file.

- Create a user account on the FTP server with the user name switch and password hello, and grant the user switch read and write permissions for the directory named Switch on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure a route exists between the switch and the PC.
Network diagram

Figure 272  Network diagram for FTP configurations: a switch operating as an FTP client

Configuration procedure

1  Configure the PC (FTP server)

Perform FTP server-related configurations on the PC, that is, create a user account on the FTP server with user name **switch** and password **hello**.

2  Configure the switch (FTP client)

# Log in to the switch. (You can log in to a switch through the Console port or by telnetting the switch. See the Login module for detailed information.)

<5500>

⚠️ **CAUTION**: If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.

# Connect to the FTP server using the `ftp` command in user view. You need to provide the IP address of the FTP server, the user name and the password as well to enter FTP view.

<5500> ftp 2.2.2.2

Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none): switch
331 Password required for switch.
Password:
230 User logged in.
[ftp]

# Enter the authorized directory on the FTP server.

[ftp] cd switch

# Execute the `put` command to upload the configuration file named `config.cfg` to the FTP server.

[ftp] put config.cfg
# Execute the `get` command to download the file named `switch.bin` to the Flash memory of the switch.

```
[ftp] get switch.bin
```

# Execute the `quit` command to terminate the FTP connection and return to user view.

```
[ftp] quit
<5500>
```

# After downloading the file, use the `boot boot-loader` command to specify the downloaded file (`switch.bin`) to be the application for next startup, and then restart the switch. Thus the switch application is upgraded.

```
<5500> boot boot-loader switch.bin
<5500> reboot
```

For information about the `boot boot-loader` command and how to specify the startup file for a switch, refer to “Basic System Configuration and Debugging” on page 929.

---

**SFTP Configuration**

Complete the tasks in Table 666 to configure SFTP.

<table>
<thead>
<tr>
<th>Item</th>
<th>Configuration task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“SFTP Configuration: A Switch Operating as an SFTP Server”</td>
<td>“Enabling an SFTP server”</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>“Configuring connection idle time”</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>“Supported SFTP client software”</td>
<td>-</td>
</tr>
<tr>
<td>“SFTP Configuration: A Switch Operating as an SFTP Client”</td>
<td>“Basic configurations on an SFTP client”</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>“Specifying the source interface or source IP address for an SFTP client”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**SFTP Configuration: A Switch Operating as an SFTP Server**

Enabling an SFTP server

Before enabling an SFTP server, you need to enable the SSH server function and specify the service type of the SSH user as SFTP or all. For details, see the SSH Server Configuration section of this manual.

**Table 667** Enable an SFTP server

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable an SFTP server</td>
<td><code>sftp server enable</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

**Configuring connection idle time**

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the
client, thus preventing a user from occupying the connection for a long time without performing any operation.

**Table 668  Configure connection idle time**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Configure the connection idle</td>
<td>ftp timeout</td>
<td>Optional 10 minutes by</td>
</tr>
<tr>
<td>time for the SFTP server</td>
<td>time-out-value</td>
<td>default</td>
</tr>
</tbody>
</table>

**Supported SFTP client software**

A Switch 5500 operating as an SFTP server can interoperate with SFTP client software, including SSH Tectia Client v4.2.0 (SFTP), v5.0, and WINSCP.

SFTP client software supports the following operations: logging in to a device; uploading a file; downloading a file; creating a directory; modify a file name or a directory name; browsing directory structure; and manually terminating a connection.

For configurations on client software, see the corresponding configuration manual.

- Currently a Switch 5500 operating as an SFTP server supports the connection of only one SFTP user. When multiple users attempt to log in to the SFTP server or multiple connections are enabled on a client, only the first user can log in to the SFTP user. The subsequent connection will fail.

- When you upload a large file through WINSCP, if a file with the same name exists on the server, you are recommended to set the packet timeout time to over 600 seconds, thus to prevent the client from failing to respond to device packets due to timeout. Similarly, when you delete a large file from the server, you are recommended to set the client packet timeout time to over 600 seconds.

**SFTP Configuration: A Switch Operating as an SFTP Client**

**Basic configurations on an SFTP client**

By default a switch can operate as an SFTP client. In this case you can connect the switch to the SFTP server to perform SFTP-related operations (such as creating/removing a directory) by executing commands on the switch. Table 669 lists the operations that can be performed on an SFTP client.

**Table 669  Basic configurations on an SFTP client**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
If you specify to authenticate a client through public key on the server, the client needs to read the local private key when logging in to the SFTP server. Since both RSA and DSA are available for public key authentication, you need to use the

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter SFTP client view</td>
<td>`sftp { host-ip</td>
<td>host-name } [ port-num ] [ identity-key { dsa</td>
</tr>
<tr>
<td>Change the working directory on the remote SFTP server</td>
<td><code>cd pathname</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Change the working directory to be the parent directory</td>
<td><code>cdup</code></td>
<td></td>
</tr>
<tr>
<td>Display the working directory on the SFTP server</td>
<td><code>pwd</code></td>
<td></td>
</tr>
<tr>
<td>Create a directory on the remote SFTP server</td>
<td><code>mkdir pathname</code></td>
<td></td>
</tr>
<tr>
<td>Remove a directory on the remote SFTP server</td>
<td><code>rmdir pathname</code></td>
<td></td>
</tr>
<tr>
<td>Delete a specified file</td>
<td><code>delete remotefile</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Query a specified file on the SFTP server</td>
<td><code>dir [ remotefile ] [ localfile ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Download a remote file from the SFTP server</td>
<td><code>get remotefile [ localfile ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Upload a local file to the remote SFTP server</td>
<td><code>put localfile [ remotefile ]</code></td>
<td></td>
</tr>
<tr>
<td>Rename a file on the remote server</td>
<td><code>rename remote-source remote-dest</code></td>
<td></td>
</tr>
<tr>
<td>Exit SFTP client view and return to system view</td>
<td><code>bye</code></td>
<td>The three commands have the same effect.</td>
</tr>
<tr>
<td>Display the online help about a specified command concerning SFTP</td>
<td>`help [ all</td>
<td>command-name ]`</td>
</tr>
</tbody>
</table>
identity-key key word to specify the algorithms to get correct local private key; otherwise you will fail to log in. For details, see SSH Operation Manual.

Specifying the source interface or source IP address for an SFTP client

You can specify the source interface or source IP address for a switch acting as an FTP client, so that it can connect to a remote SFTP server.

Table 670 Specify the source interface or source IP address for an SFTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Specify an interface as the source interface of the specified SFTP client</td>
<td>sftp source-interface interface-type interface-number</td>
<td>Use either command Not specified by default</td>
</tr>
<tr>
<td>Specify an IP address as the source IP address of the specified SFTP client</td>
<td>sftp source-ip ip-address</td>
<td></td>
</tr>
<tr>
<td>Display the source IP address used by the current SFTP client</td>
<td>display sftp source-ip</td>
<td>Optional Available in any view</td>
</tr>
</tbody>
</table>

SFTP Configuration Example

Network requirements

As shown in Figure 273, establish an SSH connection between the SFTP client (switch A) and the SFTP server (switch B). Log in to switch B through switch A to manage and transmit files. An SFTP user with the user name client001 and password abc exists on the SFTP server.

Network diagram

Figure 273 Network diagram for SFTP configuration

<table>
<thead>
<tr>
<th>SFTP Server</th>
<th>SFTP Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch B</td>
<td>Switch A</td>
</tr>
<tr>
<td>Vlan-Int1</td>
<td>Vlan-Int1</td>
</tr>
<tr>
<td>192.168.0.1/24</td>
<td>192.168.0.2/24</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure the SFTP server (switch B)

   # Create key pairs.

   `<5500> system-view
   [5500] public-key local create rsa
   [5500] public-key local create dsa`

   # Create a VLAN interface on the switch and assign to it an IP address, which is used as the destination address for the client to connect to the SFTP server.

   `[5500] interface vlan-interface 1
   [5500-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
   [5500-Vlan-interface1] quit`

   # Specify the SSH authentication mode as AAA.
SFTP Configuration

```plaintext
[5500] user-interface vty 0 4
[5500-ui-vty0-4] authentication-mode scheme

# Configure the protocol through which the remote user logs in to the switch as SSH.
[5500-ui-vty0-4] protocol inbound ssh
[5500-ui-vty0-4] quit

# Create a local user client001.
[5500] local-user client001
[5500-luser-client001] password simple abc
[5500-luser-client001] service-type ssh
[5500-luser-client001] quit

# Configure the authentication mode as password. Authentication timeout time, retry number, and update time of the server key adopt the default values.
[5500] ssh user client001 authentication-type password

# Specify the service type as SFTP.
[5500] ssh user client001 service-type sftp

# Enable the SFTP server.
[5500] sftp server enable

2  Configure the SFTP client (switch A)

# Configure the IP address of the VLAN interface on switch A. It must be in the same segment with the IP address of the VLAN interface on switch B. In this example, configure it as 192.168.0.2.

<5500> system-view
[5500] interface vlan-interface 1
[5500-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[5500-Vlan-interface1] quit

# Connect to the remote SFTP server. Enter the user name client001 and the password abc, and then enter SFTP client view.

[5500] sftp 192.168.0.1
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server’s public key?(Y/N):n
Enter password:
sftp-client>

# Display the current directory of the server. Delete the file z and verify the result.
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
```
CHAPTER 73: FTP AND SFTP CONFIGURATION

```
-rwxrwxrwx  1  noone  nogroup  225 Aug 24 08:01  pubkey2
-rwxrwxrwx  1  noone  nogroup  283 Aug 24 07:39  pubkey1
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
Received status: End of file
Received status: Success
sftp-client> delete z
The following files will be deleted:
/z
Are you sure to delete it?(Y/N): y
This operation may take a long time. Please wait...

Received status: Success
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  pubkey1
drwxrwxrwx  1  noone  nogroup  0 Sep  01 06:22  new
-rwxrwxrwx  1  noone  nogroup  225 Sep  01 06:55  pub
Received status: End of file
Received status: Success

# Add a directory new1, and then check whether the new directory is successfully created.

sftp-client> mkdir new1
Received status: Success
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  pubkey1
drwxrwxrwx  1  noone  nogroup  0 Sep  01 06:22  new
drwxrwxrwx  1  noone  nogroup  0 Sep  02 06:30  new1
Received status: End of file
Received status: Success

# Rename the directory new1 as new2, and then verify the result.

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  pubkey1
drwxrwxrwx  1  noone  nogroup  0 Sep  01 06:22  new
drwxrwxrwx  1  noone  nogroup  225 Sep  01 06:55  pub
drwxrwxrwx  1  noone  nogroup  0 Sep  02 06:33  new2
Received status: End of file
Received status: Success

# Download the file pubkey2 from the server and rename it as public.
```
SFTP Configuration

sftp-client> get pubkey2 public
This operation may take a long time, please wait...
Remote file:/pubkey2 ---> Local file: public..
Received status: End of file
Received status: Success
Downloading file successfully ended

# Upload the file pu to the server and rename it as puk, and then verify the result.
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu ---> Remote file: /puk
Received status: Success
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 pubkey1
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
Received status: End of file
Received status: Success
sftp-client>

# Exit SFTP.
sftp-client> quit
Bye
[5500]
Introduction to TFTP

Compared with FTP, TFTP (trivial file transfer protocol) features simple interactive access interface and no authentication control. Therefore, TFTP is applicable in the networks where client-server interactions are relatively simple. TFTP is implemented based on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in RFC 1986.

TFTP transmission is initiated by clients, as described in the following:

- To download a file, a client sends Read Request packets to the TFTP server, then receives data from the TFTP server, and sends acknowledgement packets to the TFTP server.
- To upload a file, a client sends Write Request packets to the TFTP server, then sends data to the TFTP server, and receives acknowledgement packets from the TFTP server.

The Switch 5500 can operate as a TFTP client only.

When Switch 5500 serving as a TFTP client downloads files from the TFTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise, and it stops rotating when the file downloading is finished, as shown in Figure 267.

When you download a file that is larger than the free space of the switch’s flash memory:

- If the TFTP server supports file size negotiation, file size negotiation will be initiated between the switch and the server and the file download operation will be aborted if the free space of the switch’s flash memory is found to be insufficient.
- If the TFTP server does not support file size negotiation, the switch will receive data from the server until the flash memory is full. If there is more data to be downloaded, the switch will prompt that the space is insufficient and delete the data partially downloaded. File download fails.

TFTP-based file transmission can be performed in the following modes:

- Binary mode for program file transfer.
- ASCII mode for text file transfer.

**Before performing TFTP-related configurations, you need to configure IP addresses for the TFTP client and the TFTP server, and make sure a route exists between the two.**
TFTP Configuration

### Table 671  TFTP configuration tasks

<table>
<thead>
<tr>
<th>Item</th>
<th>Configuration task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;TFTP Configuration: A Switch Operating as a TFTP Client&quot;</td>
<td>&quot;Basic configurations on a TFTP client&quot;</td>
<td>-</td>
</tr>
<tr>
<td>TFTP server configuration</td>
<td>For details, see the corresponding manual</td>
<td>-</td>
</tr>
</tbody>
</table>

### TFTP Configuration: A Switch Operating as a TFTP Client

#### Basic configurations on a TFTP client

By default a switch can operate as a TFTP client. In this case you can connect the switch to the TFTP server to perform TFTP-related operations (such as creating/removing a directory) by executing commands on the switch. Table 672 lists the operations that can be performed on a TFTP client.

**Table 672  Basic configurations on a TFTP client**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download a file from a TFTP server</td>
<td><code>tftp tftp-server get source-file [ dest-file ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Upload a file to a TFTP server</td>
<td><code>tftp tftp-server put source-file [ dest-file ]</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Set the file transmission mode</td>
<td>`tftp { ascii</td>
<td>binary }`</td>
</tr>
<tr>
<td>Specify an ACL rule used by the specified TFTP client to access a TFTP server</td>
<td><code>tftp-server acl acl-number</code></td>
<td>Optional Not specified by default</td>
</tr>
</tbody>
</table>

#### Specifying the source interface or source IP address for a TFTP client

You can specify the source interface and source IP address for a switch operating as a TFTP client, so that it can connect with a remote TFTP server through the IP address of the specified interface or the specified IP address.

**Table 673  Specify the source interface and source IP address for a TFTP client**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the source interface used for the current connection</td>
<td>`tftp tftp-server source-interface interface-type interface-number { get source-file [ dest-file ]</td>
<td>put source-file-url [ dest-file ] }`</td>
</tr>
<tr>
<td>Specify the source IP address used for the current connection</td>
<td>`tftp tftp-server source-ip ip-address { get source-file [ dest-file ]</td>
<td>put source-file-url [ dest-file ] }`</td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
</tbody>
</table>
The specified interface must be an existing one; otherwise a prompt appears to show that the configuration fails.

- The value of the `ip-address` argument must be an IP address on the device where the configuration is performed, and otherwise a prompt appears to show that the configuration fails.

- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between a TFTP client and a TFTP server, if you specify the source interface/source IP address only used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.

- You may specify only one source interface or source IP address for the TFTP client at one time. That is, only one of the commands `tftp source-interface` and `tftp source-ip` can be effective at one time. If both commands are configured, the one configured later will overwrite the original one.

### Table 673 Specify the source interface and source IP address for a TFTP client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify an interface as the source interface a TFTP client uses every time it connects to a TFTP server</td>
<td><code>tftp source-interface</code></td>
<td>Use either command</td>
</tr>
<tr>
<td></td>
<td><code>interface-type</code></td>
<td>Not specified by default</td>
</tr>
<tr>
<td></td>
<td><code>interface-number</code></td>
<td></td>
</tr>
<tr>
<td>Specify an IP address as the source IP address a TFTP client uses every time it connects to a TFTP server</td>
<td><code>tftp source-ip ip-address</code></td>
<td></td>
</tr>
<tr>
<td>Display the source IP address used by a TFTP client every time it connects to a TFTP server</td>
<td><code>display tftp source-ip</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in any view</td>
</tr>
</tbody>
</table>

### Network requirements

A switch operates as a TFTP client and a PC as the TFTP server. The application named `switch.bin` is stored on the PC. Download it (`switch.bin`) to the switch through TFTP, and use the `boot boot-loader` command to specify `switch.bin` as the application for next startup. Reboot the switch to upload the configuration file named `config.cfg` to the work directory on the PC to back up the configuration file.

- The TFTP working directory is configured on the TFTP server.

- Configure the IP addresses of a VLAN interface on the switch and the PC as 1.1.1.1 and 1.1.1.2 respectively. The port through which the switch connects with the PC belongs to the VLAN.

### Network diagram

**Figure 274** Network diagram for TFTP configurations
Configuration procedure

1 Configure the TFTP server (PC)

Start the TFTP server and configure the working directory on the PC.

2 Configure the TFTP client (switch).

# Log in to the switch. (You can log in to a switch through the Console port or by
telnetting the switch. See the Login module for detailed information.)

<5500>

⚠️ CAUTION: If available space on the Flash memory of the switch is not enough to
hold the file to be uploaded, you need to delete files not in use from the Flash
memory to make room for the file, and then upload the file again. The files in use
cannot be deleted. If you have to delete the files in use to make room for the file
to be uploaded, you can only delete/download them through the Boot ROM
menu.

# Enter system view

<5500> system-view

[5500]

# Configure the IP address of a VLAN interface on the switch to be 1.1.1.1, and
ensure that the port through which the switch connects with the PC belongs to
this VLAN. (This example assumes that the port belongs to VLAN 1.)

[5500] interface Vlan-interface 1
[5500-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
[5500-Vlan-interface1] quit

# Download the switch application named switch.bin from the TFTP server to the
switch.

<5500> tftp 1.1.1.2 get switch.bin switch.bin

# Upload the switch configuration file named config.cfg to the TFTP server.

<5500> tftp 1.1.1.2 put config.cfg config.cfg

# After downloading the file, use the boot boot-loader command to specify the
downloaded file (switch.bin) to be the startup file used when the switch starts the
next time, and restart the switch. Thus the switch application is upgraded.

<5500> boot boot-loader switch.bin
<5500> reboot

For information about the boot boot-loader command and how to specify the
startup file for a switch, refer to “Basic System Configuration and Debugging” on
page 929.
Information Center Overview

Introduction to Information Center
Acting as the system information hub, information center classifies and manages system information. Together with the debugging function (the `debugging` command), information center offers a powerful support for network administrators and developers in monitoring network performance and diagnosing network problems.

The information center of the system has the following features:

**Classification of system information**
The system is available with three types of information:
- Log information
- Trap information
- Debugging information

**Eight levels of system information**
The information is classified into eight levels by severity and can be filtered by level. More emergent information has a smaller severity level.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Severity value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergencies</td>
<td>1</td>
<td>The system is unavailable.</td>
</tr>
<tr>
<td>alerts</td>
<td>2</td>
<td>Information that demands prompt reaction</td>
</tr>
<tr>
<td>critical</td>
<td>3</td>
<td>Critical information</td>
</tr>
<tr>
<td>errors</td>
<td>4</td>
<td>Error information</td>
</tr>
<tr>
<td>warnings</td>
<td>5</td>
<td>Warnings</td>
</tr>
<tr>
<td>notifications</td>
<td>6</td>
<td>Normal information that needs to be noticed</td>
</tr>
<tr>
<td>informational</td>
<td>7</td>
<td>Informational information to be recorded</td>
</tr>
<tr>
<td>debugging</td>
<td>8</td>
<td>Information generated during debugging</td>
</tr>
</tbody>
</table>

Information filtering by severity works this way: information with the severity value greater than the configured threshold is not output during the filtering.
If the threshold is set to 1, only information with the severity being emergencies will be output;

If the threshold is set to 8, information of all severities will be output.

**Ten channels and six output destination of system information**

The system supports six information output destinations, including the Console, Monitor terminal (monitor), logbuffer, loghost, trapbuffer and SNMP.

The system supports ten channels. The channels 0 through 5 have their default channel names and are associated with six output destinations by default. Both the channel names and the associations between the channels and output destinations can be changed through commands.

**Table 675 Information channels and output destinations**

<table>
<thead>
<tr>
<th>Information channel number</th>
<th>Default channel name</th>
<th>Default output destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>console</td>
<td>Console (Receives log, trap and debugging information)</td>
</tr>
<tr>
<td>1</td>
<td>monitor</td>
<td>Monitor terminal (Receives log, trap and debugging information, facilitating remote maintenance)</td>
</tr>
<tr>
<td>2</td>
<td>loghost</td>
<td>Log host (Receives log, trap and debugging information and information will be stored in files for future retrieval)</td>
</tr>
<tr>
<td>3</td>
<td>trapbuffer</td>
<td>Trap buffer (Receives trap information, a buffer inside the device for recording information)</td>
</tr>
<tr>
<td>4</td>
<td>logbuffer</td>
<td>Log buffer (Receives log information, a buffer inside the device for recording information)</td>
</tr>
<tr>
<td>5</td>
<td>snmpagent</td>
<td>SNMP NMS (Receives trap information)</td>
</tr>
<tr>
<td>6</td>
<td>channel6</td>
<td>Not specified (Receives log, trap, and debugging information)</td>
</tr>
<tr>
<td>7</td>
<td>channel7</td>
<td>Not specified (Receives log, trap, and debugging information)</td>
</tr>
<tr>
<td>8</td>
<td>channel8</td>
<td>Not specified (Receives log, trap, and debugging information)</td>
</tr>
<tr>
<td>9</td>
<td>channel9</td>
<td>Not specified (Receives log, trap, and debugging information)</td>
</tr>
</tbody>
</table>

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 information can be classified by source module and then filtered. Some module names and description are shown in Table 676.

<table>
<thead>
<tr>
<th>Module name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8021X</td>
<td>802.1x module</td>
</tr>
<tr>
<td>ACL</td>
<td>Access control list module</td>
</tr>
<tr>
<td>ADBM</td>
<td>Address base module</td>
</tr>
<tr>
<td>AM</td>
<td>Access management module</td>
</tr>
<tr>
<td>ARP</td>
<td>Address resolution protocol module</td>
</tr>
<tr>
<td>CMD</td>
<td>Command line module</td>
</tr>
<tr>
<td>DEV</td>
<td>Device management module</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic host configuration protocol module</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name system module</td>
</tr>
<tr>
<td>ETH</td>
<td>Ethernet module</td>
</tr>
<tr>
<td>FIB</td>
<td>Forwarding module</td>
</tr>
<tr>
<td>FTM</td>
<td>Fabric topology management module</td>
</tr>
<tr>
<td>FTMCMD</td>
<td>Fabric topology management command module</td>
</tr>
<tr>
<td>FTPS</td>
<td>FTP server module</td>
</tr>
<tr>
<td>HA</td>
<td>High availability module</td>
</tr>
<tr>
<td>HABP</td>
<td>3Com authentication bypass protocol module</td>
</tr>
<tr>
<td>HTTPD</td>
<td>HTTP server module</td>
</tr>
<tr>
<td>HWCM</td>
<td>3Com Configuration Management private MIB module</td>
</tr>
<tr>
<td>IFNET</td>
<td>Interface management module</td>
</tr>
<tr>
<td>IGSP</td>
<td>IGMP snooping module</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol module</td>
</tr>
<tr>
<td>LAGG</td>
<td>Link aggregation module</td>
</tr>
<tr>
<td>LINE</td>
<td>Terminal line module</td>
</tr>
<tr>
<td>MSTP</td>
<td>Multiple spanning tree protocol module</td>
</tr>
<tr>
<td>MTRACE</td>
<td>Multicast traceroute query module</td>
</tr>
<tr>
<td>NAT</td>
<td>Network address translation module</td>
</tr>
<tr>
<td>NDP</td>
<td>Neighbor discovery protocol module</td>
</tr>
<tr>
<td>NTDP</td>
<td>Network topology discovery protocol module</td>
</tr>
<tr>
<td>NTP</td>
<td>Network time protocol module</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open shortest path first module</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure module</td>
</tr>
<tr>
<td>RDS</td>
<td>Radius module</td>
</tr>
<tr>
<td>RMON</td>
<td>Remote monitor module</td>
</tr>
<tr>
<td>RSA</td>
<td>Revest, Shamir and Adleman encryption module</td>
</tr>
<tr>
<td>SHELL</td>
<td>User interface module</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple network management protocol module</td>
</tr>
<tr>
<td>SOCKET</td>
<td>Socket module</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure shell module</td>
</tr>
</tbody>
</table>
To sum up, the major task of the information center is to output the three types of information of the modules onto the ten channels in terms of the eight severity levels and according to the user’s settings, and then redirect the system information from the ten channels to the six output destinations.

**System Information Format**

System information has the following format:

```
<priority>timestamp sysname module/level/digest:content
```

- The closing set of angel brackets < >, the space, the forward slash /, and the colon are all required in the above format.
- Before the <priority> may have %, #, or * followed with a space, indicating log, alarm, or debugging information respectively.

Below is an example of the format of log information to be output to a log host:

```
% <188>Dec  6 10:44:55:283 2006 3Com NTP/5/NTP_LOG:- 1 - NTP service enable
```

(-1- indicates that the unit number of the device is 1.)

What follows is a detailed explanation of the fields involved:

**Priority**

The priority is calculated using the following formula: facility*8+severity-1, in which

- facility (the device name) defaults to local7 with the value being 23 (the value of local6 is 22, that of local5 is 21, and so on).
- severity (the information level) ranges from 1 to 8. Table 674 details the value and meaning associated with each severity.

Note that there is no space between the priority and timestamp fields and the priority field appears 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.

Note that there is a space between the timestamp and sysname (host name) fields.

<table>
<thead>
<tr>
<th>Module name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSMIB</td>
<td>System MIB module</td>
</tr>
<tr>
<td>TAC</td>
<td>HWTACACS module</td>
</tr>
<tr>
<td>TELNET</td>
<td>Telnet module</td>
</tr>
<tr>
<td>TFTPC</td>
<td>TFTP client module</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual local area network module</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual router redundancy protocol module</td>
</tr>
<tr>
<td>VTY</td>
<td>Virtual type terminal module</td>
</tr>
<tr>
<td>XM</td>
<td>XModem module</td>
</tr>
<tr>
<td>default</td>
<td>Default settings for all the modules</td>
</tr>
</tbody>
</table>
The time stamp is in the format of `Mmm dd hh:mm:ss:ms yyyy`.

Each field is described as follows:

- **Mmm** represents the month, and the available values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

- **dd** is the date, which shall follow a space if less than 10, for example, 7.

- **hh:mm:ss:ms** is the local time, where **hh** is in the 24-hour format, ranging from 00 to 23, both **mm** and **ss** range from 00 to 59, **ms** ranges from 000 to 999.

- **yyyy** is the year.

**Sysname**

Sysname is the system name of the local switch and defaults to 5500.

You can use the **sysname** command to modify the system name. Refer to “Basic System Configuration and Debugging” on page 929.

Note that there is a space between the sysname and module fields.

**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. Refer to Table 676 for module name and description.

Between **module** and **level** is a /.

**Level (Severity)**

System information can be divided into eight levels based on its severity, from 1 to 8. Refer to Table 674 for definition and description of these severity levels. Note that there is a forward slash / between the level (severity) and digest fields.

**Digest**

The digest field is a string of up to 32 characters, outlining the system information.

Note that there is a colon between the digest and content fields.

**Content**

This field provides the content of the system information.

><i>The above section describes the log information format sent to a log host by a switch. Some log host software will resolve the received information as well as its format, so that you may see the log format displayed on the log host is different from the one described in this manual.</i>
**Information Center Configuration**

**Introduction to the Information Center Configuration Tasks**

**Table 677** Information center configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring Synchronous Information Output”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to the Console”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to a Monitor Terminal”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to a Log Host”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to the Trap Buffer”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to the Log Buffer”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Setting to Output System Information to the SNMP NMS”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**Configuring Synchronous Information Output**

Synchronous information output refers to the feature that if the system information such as log, trap, or debugging information is output when the user is inputting commands, the command line prompt (in command editing mode a prompt, or a [Y/N] string in interaction mode) and the input information are echoed after the output.

This feature is used in the case that your input is interrupted by a large amount of system output. With this feature enabled, the system echoes your previous input and you can continue your operations from where you were stopped.

**Table 678** Configure synchronous information output

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable synchronous information output</td>
<td>info-center synchronous</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default</td>
</tr>
</tbody>
</table>

- *If the system information is output before you input any information following the current command line prompt, the system does not echo any command line prompt after the system information output.*
- *In the interaction mode, you are prompted for some information input. If the input is interrupted by system output, no system prompt (except the Y/N string) will be echoed after the output, but your input will be displayed in a new line.*
Setting to output system information to the console

Table 679  Set to output system information to the console

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the information center</td>
<td>info-center enable</td>
<td>Optional</td>
</tr>
<tr>
<td>Enable system information output</td>
<td>info-center console channel</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>{ channel-number</td>
<td>channel-name }</td>
</tr>
<tr>
<td>Configure the output rules of</td>
<td>info-center source {</td>
<td>Optional</td>
</tr>
<tr>
<td>system information</td>
<td>modu-name</td>
<td>default } channel { channel-number</td>
</tr>
<tr>
<td>Set the format of time stamp in</td>
<td>info-center timestamp { log</td>
<td>Optional</td>
</tr>
<tr>
<td>the output information</td>
<td></td>
<td>trap</td>
</tr>
</tbody>
</table>

To view the debugging information of some modules on the switch, you need to set the type of the output information to debug when configuring the system information output rules, and use the debugging command to enable debugging for the corresponding modules.

Table 680  Default output rules for different output destinations

<table>
<thead>
<tr>
<th>Output destination</th>
<th>Modules allowed</th>
<th>LOG</th>
<th>TRAP</th>
<th>DEBUG</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Enable/</td>
<td>Enable/</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disab</td>
<td>disabled</td>
<td>disabl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ted</td>
<td></td>
<td>d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severit</td>
<td>Severity</td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console</td>
<td>default (all</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>warnings</td>
<td>debuggin</td>
<td>debugging</td>
</tr>
<tr>
<td>Monitor terminal</td>
<td>default (all</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>warnings</td>
<td>debuggin</td>
<td>debugging</td>
</tr>
<tr>
<td>Log host</td>
<td>default (all</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>informational</td>
<td>debuggin</td>
<td>debugging</td>
</tr>
<tr>
<td>Trap buffer</td>
<td>default (all</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>warning</td>
<td>warnings</td>
<td>debugging</td>
</tr>
<tr>
<td>Log buffer</td>
<td>default (all</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>debuggi</td>
<td>warnings</td>
<td>debugging</td>
</tr>
<tr>
<td>SNMP NMS</td>
<td>default (all</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>modules)</td>
<td>debuggi</td>
<td>warnings</td>
<td>debugging</td>
</tr>
</tbody>
</table>

Enabling system information display 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.
Make sure that the debugging/log/trap information terminal display function is enabled (use the `terminal monitor` command) before you enable the corresponding terminal display function by using the `terminal debugging`, `terminal logging`, or `terminal trapping` command.

### Setting to Output 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, TTY, or VTY user interface.

#### Setting to output system information to a monitor terminal

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Enable the information center</td>
<td><code>info-center enable</code></td>
<td>Optional&lt;br&gt;Enabled by default.</td>
</tr>
<tr>
<td>Enable system information output to Telnet terminal or dumb terminal</td>
<td>`info-center monitor channel { channel-number</td>
<td>channel-name }`</td>
</tr>
<tr>
<td>Configure the output rules of system information</td>
<td>`info-center source { modu-name</td>
<td>default } channel { channel-number</td>
</tr>
<tr>
<td>Set the format of time stamp in the output information</td>
<td>`info-center timestamp { log</td>
<td>trap</td>
</tr>
</tbody>
</table>

- When there are multiple Telnet users or dumb terminal users, they share some configuration parameters including module filter, language and severity level threshold. In this case, change to any such parameter made by one user will also be reflected on all other user terminals.
To view debugging information of specific modules, you need to set the information type as **debug** when setting the system information output rules, and enable debugging for corresponding modules through the **debugging** command.

**Enabling system information display 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.

**Table 683** Enable the display of system information on a monitor terminal

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the debugging/log/trap information</td>
<td>terminal monitor</td>
<td>Optional</td>
</tr>
<tr>
<td>terminal display function</td>
<td>terminal debugging</td>
<td>Optional</td>
</tr>
<tr>
<td>Enable debugging information terminal display</td>
<td>terminal logging</td>
<td>Optional</td>
</tr>
<tr>
<td>function</td>
<td>terminal trapping</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

**Setting to Output System Information to a Log Host**

**Table 684** Set to output system information to a log host

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the information center</td>
<td>info-center enable</td>
<td>Optional</td>
</tr>
<tr>
<td>Enable information output for a specified</td>
<td>info-center switch-on</td>
<td>Optional</td>
</tr>
<tr>
<td>switch in a fabric</td>
<td>{ unit</td>
<td>By default, debugging information</td>
</tr>
<tr>
<td></td>
<td>unit-id</td>
<td>master</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**Table 684**  Set to output system information to a log host

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable system information output to a log host</td>
<td>info-center loghost host-ip-addr [ channel { channel-number</td>
<td>channel-name }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the switch does not output information to the log host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After you configure the switch to output information to the log host, the switch uses information channel 2 by default.</td>
</tr>
<tr>
<td>Configure the source interface through which log information is sent to the log host</td>
<td>info-center loghost source interface-type interface-number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source interface is configured, and the system automatically selects an interface as the source interface.</td>
</tr>
<tr>
<td>Configure the output rules of system information</td>
<td>info-center source { modu-name</td>
<td>default } channel { channel-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to Table 680 for the default output rules of system information.</td>
</tr>
<tr>
<td>Set the format of the time stamp to be sent to the log host</td>
<td>info-center timestamp loghost ( date</td>
<td>no-year-date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the time stamp format of the information output to the log host is <strong>date</strong>.</td>
</tr>
</tbody>
</table>

- **After the switches form a fabric, you can use the** info-center switch-on **command to enable the information output for the switches to make the log, debugging and trap information of each switch in the fabric synchronous. Each switch sends its own information to other switches in the fabric and receives information sent by other switches at the same time to update the information on itself. In this way, the switch ensures the synchronization of log, debugging and trap information in the whole fabric.**

- **Be sure to set the correct IP address when using the** info-center loghost **command. A loopback IP address will cause an error message prompting that this address is invalid.**

### Setting to Output System Information to the Trap Buffer

**Table 685**  Set to output system information to the trap buffer

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the information center</td>
<td>info-center enable</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enabled by default.</td>
</tr>
<tr>
<td>Enable system information output to the trap buffer</td>
<td>info-center trapbuffer [channel { channel-number</td>
<td>channel-name }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the switch uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default.</td>
</tr>
</tbody>
</table>
Setting to Output System Information to the Log Buffer

<table>
<thead>
<tr>
<th>Table 685</th>
<th>Set to output system information to the trap buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
</tbody>
</table>
| Configure the output rules of system information | `info-center source { modu-name | default } channel { channel-number | channel-name } { (log | trap | debug) { (level severity | state state }) }*` | Optional
| | | Refer to Table 680 for the default output rules of system information. |
| Set the format of time stamp in the output information | `info-center timestamp { log | trap | debugging } { boot | date | none }` | Optional
| | | By default, the time stamp format of the output trap information is **date**. |

Setting to Output System Information to the SNMP NMS

<table>
<thead>
<tr>
<th>Table 686</th>
<th>Set to output system information to the log buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| Enable the information center | `info-center enable` | Optional
| | | Enabled by default. |
| Enable information output to the log buffer | `info-center logbuffer { channel { channel-number | channel-name } | size buffersize }*` | Optional
| | | By default, the switch uses information channel 4 to output log information to the log buffer, which can hold up to 512 items by default. |
| Configure the output rules of system information | `info-center source { modu-name | default } channel { channel-number | channel-name } { (log | trap | debug) { (level severity | state state }) }*` | Optional
| | | Refer to Table 680 for the default output rules of system information. |
| Set the format of time stamp in the output information | `info-center timestamp { log | trap | debugging } { boot | date | none }` | Optional
| | | By default, the time stamp format of the output log information is **date**. |

Table 687 | Set to output system information to the SNMP NMS |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| Enable the information center | `info-center enable` | Optional
| | | Enabled by default. |
| Enable information output to the SNMP NMS | `info-center snmp channel { channel-number | channel-name }` | Optional
| | | By default, the switch outputs trap information to SNMP through channel 5. |
| Configure the output rules of system information | `info-center source { modu-name | default } channel { channel-number | channel-name } { (log | trap | debug) { (level severity | state state }) }*` | Optional
| | | Refer to Table 680 for the default output rules of system information. |
To send information to a remote SNMP NMS properly, related configurations are required on both the switch and the SNMP NMS.

Displaying and Maintaining Information Center

After completing the above configuration, you can execute the `display` commands in any view to display the running status of the information center, and thus validate your configurations. You can also execute the `reset` commands in user view to clear the information in the log buffer and trap buffer.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information on an information channel</td>
<td>`display channel [channel-number</td>
<td>channel-name]`</td>
</tr>
<tr>
<td>Display the operation status of information center, the configuration of information channels, the format of time stamp and the information output in case of fabric</td>
<td><code>display info-center [unit unit-id]</code></td>
<td></td>
</tr>
<tr>
<td>Display the status of log buffer and the information recorded in the log buffer</td>
<td><code>display logbuffer [unit unit-id] [level severity] [size buffersize]</code>* [ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display the summary information recorded in the log buffer</td>
<td><code>display logbuffer summary [level severity]</code></td>
<td></td>
</tr>
<tr>
<td>Display the status of trap buffer and the information recorded in the trap buffer</td>
<td><code>display trapbuffer [unit unit-id] [size buffersize]</code></td>
<td></td>
</tr>
<tr>
<td>Clear information recorded in the log buffer</td>
<td><code>reset logbuffer [unit unit-id]</code></td>
<td>Available in user view</td>
</tr>
<tr>
<td>Clear information recorded in the trap buffer</td>
<td><code>reset trapbuffer [unit unit-id]</code></td>
<td></td>
</tr>
</tbody>
</table>

Information Center Configuration Examples

Log Output to a UNIX Log Host

The switch sends the following log information to the Unix log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than informational.
Network diagram

Figure 275 Network diagram for log output to a Unix log host

![Network diagram](image)

Configuration procedure

1. Configure the switch:

   # Enable the information center.
   
   <Switch> system-view
   [Switch] info-center enable
   
   # Disable the function of outputting information to log host channels.
   
   [Switch] undo info-center source default channel loghost
   
   # Configure the host whose IP address is 202.38.1.10 as the log host. Permit ARP and IP modules to output information with severity level higher than informational to the log host.
   
   [Switch] info-center loghost 202.38.1.10 facility local4
   [Switch] info-center source arp channel loghost log level informational debug state off trap state off
   [Switch] info-center source ip channel loghost log level informational debug state off trap state off

2. Configure the log host:

   The operations here are performed on SunOS 4.0. The operations on other manufacturers’ Unix operation systems are similar.

   Step 1: Execute the following commands as the super user (root user).
   
   # mkdir /var/log/Switch
   # touch /var/log/Switch/information

   Step 2: Edit the file `/etc/syslog.conf` as the super user (root user) to add the following selector/action pairs.
   
   # Switch configuration messages
   local4.info /var/log/Switch/information

   When you edit the file `/etc/syslog.conf`, note that:
   
   ■ A note must start in a new line, starting with a `#` sign.
   ■ In each pair, a tab should be used as a separator instead of a space.
   ■ No space is allowed at the end of a file name.
   ■ The device name (facility) and received log information severity level specified in the file `/etc/syslog.conf` must be the same as those corresponding parameters configured in the commands `info-center loghost` and `info-center source`. Otherwise, log information may not be output to the log host normally.

   Step 3: After the log file `information` is created and the file `/etc/syslog.conf` is modified, execute the following command to send a HUP signal to the system daemon `syslogd`, so that it can reread its configuration file `/etc/syslog.conf`. 
# ps -ae | grep syslogd
147
# kill -HUP 147

After all the above operations, the switch can make records in the corresponding log file.

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file syslog.conf, you can sort information precisely for filtering.

Log Output to a Linux Log Host

Network requirements
The switch sends the following log information to the Linux log host whose IP address is 202.38.1.10: All modules’ log information, with severity higher than errors.

Network diagram

Figure 276 Network diagram for log output to a Linux log host

Configuration procedure

1 Configure the switch:
   # Enable the information center.
   <Switch> system-view
   [Switch] info-center enable
   # Configure the host whose IP address is 202.38.1.10 as the log host. Permit all modules to output log information with severity level higher than error to the log host.
   [Switch] info-center loghost 202.38.1.10 facility local7
   [Switch] info-center source default channel loghost log level errors debug state off trap state off

2 Configure the log host:
   Step 1: Execute the following commands as a super user (root user).
   # mkdir /var/log/Switch
   # touch /var/log/Switch/information
   Step 2: Edit the file /etc/syslog.conf as the super user (root user) to add the following selector/action pairs.
   # Switch configuration messages
   local7.info /var/log/Switch/information

   Note the following items when you edit file /etc/syslog.conf:
   - A note must start in a new line, starting with a # sign.
   - In each pair, a tab should be used as a separator instead of a space.
No space is permitted at the end of the file name.

The device name (facility) and received log information severity specified in file /etc/syslog.conf must be the same with those corresponding parameters configured in commands info-center loghost and info-center source. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file information is created and the file /etc/syslog.conf is modified, execute the following commands to view the process ID of the system daemon syslogd, stop the process, and then restart the daemon syslogd in the background with the -r option.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

In case of Linux log host, the daemon syslogd must be started with the -r option.

After all the above operations, the switch can record information in the corresponding log file.

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file syslog.conf, you can sort information precisely for filtering.

Log Output to the Console

Network requirements
The switch sends the following information to the console: the log information of the two modules ARP and IP, with severity higher than informational.

Network diagram

Figure 277 Network diagram for log output to the console

Configuration procedure

# Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

# Disable the function of outputting information to the console channels.

```
[Switch] undo info-center source default channel console
```

# Enable log information output to the console. Permit ARP and IP modules to output log information with severity level higher than informational to the console.

```
[Switch] info-center console channel console
[Switch] info-center source arp channel console log level informational debug state off trap state off
[Switch] info-center source ip channel console log level informational debug state off trap state off
```
# Enable terminal display.

<Switch> terminal monitor
<Switch> terminal logging
Traditionally, switch software is loaded through a serial port. This approach is slow, time-consuming and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can load/download software/files conveniently to the switch through an Ethernet port.

This chapter introduces how to load the Boot ROM and host software to a switch locally and remotely.

### Introduction to Loading Approaches

You can load software locally by using:
- XModem through Console port
- TFTP through Ethernet port
- FTP through Ethernet port

You can load software remotely by using:
- FTP
- TFTP

*The Boot ROM software version should be compatible with the host software version when you load the Boot ROM and host software.*

### Local Boot ROM and Software Loading

If your terminal is directly connected to the switch's console port, you can load the Boot ROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch.

*The loading process of the Boot ROM software is the same as that of the host software, except that during the former process, you should press 6 or <Ctrl+U> and <Enter> after entering the BOOT menu and the system gives different prompts. The following text mainly describes the Boot ROM loading process.*

### BOOT Menu

```
Starting......
```

```
***********************************************************
* 3Com Switch 5500-EI 52-Port BOOTROM, Version 507*
***********************************************************
```
Press Ctrl-B to enter Boot Menu... 

Press <Ctrl+B>. The system displays:

Password:

To enter the BOOT menu, you should press <Ctrl+B> within five seconds after the information Press Ctrl-B to enter BOOT Menu... displays. Otherwise, the system starts to extract the program; and if you want to enter the BOOT Menu at this time, you will have to restart the switch.

Enter the correct Boot ROM password (no password is set by default). The system enters the BOOT Menu:

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9):

Loading Software Using XModem through the Console Port

Introduction to XModem

XModem protocol is a file transfer protocol that is widely used due to its simplicity and high stability. The XModem protocol transfers files through Console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and multiple attempts of error packet retransmission (generally the maximum number of retransmission attempts is ten).

The XModem transmission procedure is completed by a receiving program and a sending program. The receiving program sends negotiation characters to negotiate a packet checking method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends acknowledgement characters and the sending program proceeds to send another packet. If the check fails, the receiving program sends negative acknowledgement characters and the sending program retransmits the packet.
Loading Boot ROM

Follow these steps to load the Boot ROM:

1. At the prompt **Enter your choice(0-9):** in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the Boot ROM update menu shown below:

   Bootrom update menu:
   1. Set TFTP protocol parameter
   2. Set FTP protocol parameter
   3. Set XMODEM protocol parameter
   0. Return to boot menu

   Enter your choice(0-3):

2. Press 3 in the above menu to download the Boot ROM using XModem. The system displays the following setting menu for download baudrate:

   Please select your download baudrate:
   1. * 9600
   2. 19200
   3. 38400
   4. 57600
   5. 115200
   0. Return

   Enter your choice (0-5):

3. Choose an appropriate baud rate for downloading. For example, if you press 5, the baud rate 115200 bps is chosen and the system displays the following information:

   Download baudrate is 115200 bit/s
   Please change the terminal’s baudrate to 115200 bit/s and select XMODEM protocol
   Press enter key when ready

   * If you have chosen 9600 bps as the download baud rate, you need not modify the HyperTerminal’s baud rate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

   Following are configurations on PC. Take the HyperTerminal in Windows 2000 as an example.

4. Choose [File/Properties] in HyperTerminal, click <Configure> in the pop-up dialog box, and then select the baudrate of 115200 bps in the Console port configuration dialog box that appears, as shown in Figure 278, Figure 279.
Figure 278  Properties dialog box

Figure 279  Console port configuration dialog box
5 Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 280.

**Figure 280** Connect and disconnect buttons

![Connect and disconnect buttons](image)

---

*The new baudrate takes effect after you disconnect and reconnect the HyperTerminal program.*

6 Press <Enter> to start downloading the program. The system displays the following information:

Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCC

7 Choose [Transfer/Send File] in HyperTerminal, and click <Browse> in pop-up dialog box, as shown in Figure 281. Select the software file that you need to load to the switch, and set the protocol to XModem.

**Figure 281** Send file dialog box

![Send file dialog box](image)

8 Click <Send>. The system displays the page, as shown in Figure 282.
After the sending process completes, the system displays the following information:

```
Loading ...CCCCCCCCC done!
```

Step 10: Reset HyperTerminal’s baudrate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....................................done!
```

- If the HyperTerminal’s baudrate is not reset to 9600 bps, the system prompts **Your baudrate should be set to 9600 bps again! Press enter key when ready.**
- You need not reset the HyperTerminal’s baudrate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades the Boot ROM automatically and prompts **Bootrom updating now..............................done!**

### Loading host software

Follow these steps to load the host software:

1. Select <1> in BOOT Menu and press <Enter>. The system displays the following information:
   1. Set TFTP protocol parameter
   2. Set FTP protocol parameter
   3. Set XMODEM protocol parameter
   0. Return to boot menu

   Enter your choice (0-3):

2. Enter 3 in the above menu to load the host software by using XModem.

---

**Figure 282** Sending file page

<table>
<thead>
<tr>
<th>Sending:</th>
<th>D:\version\switch.btm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet:</td>
<td>12</td>
</tr>
<tr>
<td>Error checking:</td>
<td>CRC</td>
</tr>
<tr>
<td>Retries:</td>
<td>0</td>
</tr>
<tr>
<td>Total retries:</td>
<td>0</td>
</tr>
<tr>
<td>Last error:</td>
<td></td>
</tr>
<tr>
<td>File:</td>
<td></td>
</tr>
<tr>
<td>Elapsed:</td>
<td>00:00:01</td>
</tr>
<tr>
<td>Remaining:</td>
<td></td>
</tr>
<tr>
<td>Throughput:</td>
<td></td>
</tr>
</tbody>
</table>

**Xmodem file send for switch**
The subsequent steps are the same as those for loading the Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.

You can also use the `xmodem get` command to load host software through the Console port (of AUX type). The load procedures are as follows (assume that the PC is connected to the Console port of the switch, and logs onto the switch through the Console port):

1. Execute the `xmodem get` command in user view. In this case, the switch is ready to receive files.
2. Enable the HyperTerminal on the PC, and configure XModem as the transfer protocol, and configure communication parameters on the Hyper Terminal the same as that on the Console port.
3. Choose the file to be loaded to the switch, and then start to transmit the file.

### Loading by TFTP through Ethernet Port

**Introduction to TFTP**

TFTP, a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It is over UDP to provide unreliable data stream transfer service.

### Loading the Boot ROM

**Figure 283**  Local loading using TFTP

1. As shown in Figure 283, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.

   **CAUTION:** TFTP server program is not provided with the 3Com Series Ethernet Switches.

2. Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

3. Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

   At the prompt **Enter your choice(0-9):** in the BOOT Menu, press `<6>` or `<Ctrl+U>`, and then press `<Enter>` to enter the Boot ROM update menu shown below:

   **Bootrom update menu:**
   1. Set TFTP protocol parameter
   2. Set FTP protocol parameter
   3. Set XMODEM protocol parameter
   0. Return to boot menu

   **Enter your choice(0-3):**
4 Enter 1 in the above menu to download the Boot ROM using TFTP. Then set the following TFTP-related parameters as required:

- Load File name: s4f04_02.btm
- Switch IP address: 1.1.1.2
- Server IP address: 1.1.1.1

5 Press <Enter>. The system displays the following information:

Are you sure to update your bootrom?Yes or No(Y/N)

6 Enter Y to start file downloading or N to return to the Boot ROM update menu. If you enter Y, the system begins to download and update the Boot ROM. Upon completion, the system displays the following information:

Loading........................................done
Bootrom updating............done!

**Loading host software**

Follow these steps to load the host software.

1 Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):3

2 Enter 1 in the above menu to download the host software using TFTP.

The subsequent steps are the same as those for loading the Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.

**CAUTION:** When loading Boot ROM and host software using TFTP through BOOT menu, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.

---

**Loading by FTP through Ethernet Port**

**Introduction to FTP**

FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

**Loading Procedure Using FTP Client**

- Loading Boot ROM
As shown in Figure 284, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC. You can use one computer as both configuration device and FTP server.

1. Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.

2. Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

At the prompt Enter your choice(0-9): in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the Boot ROM update menu shown below:

Bootrom update menu:
1. Set TFTP protocol parameter 
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):

4. Enter 2 in the above menu to download the Boot ROM using FTP. Then set the following FTP-related parameters as required:

   Load File name: s4f04.btm
   Switch IP address: 10.1.1.2
   Server IP address: 10.1.1.1
   FTP User Name: 3600
   FTP User Password: abc

5. Press <Enter>. The system displays the following information:

   Are you sure to update your bootrom? Yes or No(Y/N)

6. Enter Y to start file downloading or N to return to the Boot ROM update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

   Loading........................................done
   Bootrom updating...........done!
   ■ Loading host software

Follow these steps to load the host software:

1. Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

   1. Set TFTP protocol parameter
   2. Set FTP protocol parameter
   3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice (0-3):

Enter 2 in the above menu to download the host software using FTP.

The subsequent steps are the same as those for loading the Boot ROM, except for that the system gives the prompt for host software loading instead of Boot ROM loading.

**CAUTION: When loading the Boot ROM and host software using FTP through BOOT menu, you are recommended to use the PC directly connected to the device as FTP server to promote upgrading reliability.**

### Remote Boot ROM and Software Loading

If your terminal is not directly connected to the switch, you can telnet to the switch, and use FTP or TFTP to load the Boot ROM and host software remotely.

#### Remote Loading Using FTP

##### Loading Procedure Using FTP Client

1. **Loading the Boot ROM**

   As shown in Figure 285, a PC is used as both the configuration device and the FTP server. You can telnet to the switch, and then execute the FTP commands to download the Boot ROM program s4f04.btm from the remote FTP server (whose IP address is 10.1.1.1) to the switch.

   ![Figure 285: Remote loading using FTP Client](image)

   **a** Download the program to the switch using FTP commands.

   ```
   <5500> ftp 10.1.1.1
   Trying ...
   Press CTRL+K to abort
   Connected.
   220 WFTPD 2.0 service (by Texas Imperial Software) ready for new use
   r
   User (none): abc
   331 Give me your password, please
   Password:
   230 Logged in successfully
   [ftp] get s4f04.btm
   [ftp] bye
   ```

   **i** When using different FTP server software on PC, different information will be output to the switch.

   **b** Update the Boot ROM program on the switch.

   ```
   <5500> boot bootrom s4f04.btm
   This will update BootRom file on unit 1. Continue? [Y/N] y
   ```
Remote Boot ROM and Software Loading

Upgrading BOOTROM, please wait...
Upgrade BOOTROM succeeded!

c Restart the switch.

Before restarting the switch, make sure you have saved all other configurations that you want, so as to avoid losing configuration information.

2 Loading host software

Loading the host software is the same as loading the Boot ROM program, except that the file to be downloaded is the host software file, and that you need to use the `boot boot-loader` command to select the host software used for next startup of the switch.

After the above operations, the Boot ROM and host software loading is completed.

Pay attention to the following:

- The loading of Boot ROM and host software takes effect only after you restart the switch with the `reboot` command.
- If the space of the Flash memory is not enough, you can delete the unused files in the Flash memory before software downloading. For information about deleting files, refer to “File System Management Configuration” on page 867.
- Ensure that the power supply is available during software loading.

Loading Procedure Using FTP Server

As shown in Figure 286, the switch is used as the FTP server. You can telnet to the switch, and then execute the FTP commands to upload the Boot ROM s4f04.btm to the switch.

1 Loading the Boot ROM

Figure 286 Remote loading using FTP server

As shown in Figure 286, connect the switch through an Ethernet port to the PC (whose IP address is 10.1.1.1)

b Configure the IP address of VLAN-interface 1 on the switch to 192.168.0.39, and subnet mask to 255.255.255.0.

You can configure the IP address for any VLAN on the switch for FTP transmission. However, before configuring the IP address for a VLAN interface, you have to make sure whether the IP addresses of this VLAN and PC are routable.

<5500> system-view
System View: return to User View with Ctrl+Z.
[5500] interface Vlan-interface 1
[5500-Vlan-interface1] ip address 192.168.0.39 255.255.255.0
c Enable FTP service on the switch, and configure the FTP user name to test and password to pass.

```
[5500-Vlan-interface1] quit
[5500] ftp server enable
[5500] local-user test
New local user added.
[5500-luser-test] password simple pass
[5500-luser-test] service-type ftp
```

d Enable FTP client software on the PC. Refer to Figure 287 for the command line interface in Windows operating system.

**Figure 287** Command line interface

```
C:\\WINDO\\system32\\cmd.exe
```

e Use the `cd` command on the interface to enter the path that the Boot ROM upgrade file is to be stored. Assume the name of the path is D:Bootrom, as shown in Figure 288.
Figure 288  Enter Boot ROM directory

```
C:\d:
D:\cd Bootrom
D:\Bootrom>
```

f  Enter `ftp 192.168.0.39` and enter the user name test, password pass, as shown in Figure 289, to log on to the FTP server.

Figure 289  Log on to the FTP server

```
C:\d:
D:\cd Bootrom
D:\Bootrom>ftp 192.168.0.39
Connected to 192.168.0.39.
220 FTP service ready.
User (192.168.0.39:<none>): test
331 Password required for test.
Password:
230 User logged in.
Ftp>
```

g  Use the `put` command to upload the file s4f04.btm to the switch, as shown in Figure 290.
Figure 290  Upload file 4f04.btm to the switch

h  Configure s4f04.btm to be the Boot ROM at next startup, and then restart the switch.

<5500> boot bootrom s4f04.btm
  This will update Bootrom on unit 1.  Continue? [Y/N] y
  Upgrading Bootrom, please wait...
  Upgrade Bootrom succeeded!

<5500> reboot

After the switch restarts, the file s4f04.btm is used as the Boot ROM. It indicates that the Boot ROM loading is finished.

2  Loading host software

Loading the host software is the same as loading the Boot ROM program, except that the file to be downloaded is the host software file, and that you need to use the boot boot-loader command to select the host software used for the next startup of the switch.

Only the configuration steps concerning loading are listed here. For detailed description of the corresponding configuration commands, refer to the “FTP and SFTP Configuration” on page 875 and “TFTP Configuration” on page 895.

Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP. The only difference is that TFTP is used to load software to the switch, and the switch can only act as a TFTP client.
# Basic System Configuration and Debugging

## Basic System Configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the current date and time of the system</td>
<td><code>clock datetime HH:MM:SS</code> { YYYY/MM/DD</td>
<td>MM/DD/YYYY }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute this command in user view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 23:55:00 04/01/2000 when the system starts up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Set the local time zone</td>
<td><code>clock timezone zone-name</code> { add</td>
<td>minus } <code>HH:MM:SS</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, it is the UTC time zone.</td>
</tr>
<tr>
<td>Set the name and time range of the summer time</td>
<td><code>clock summer-time zone_name</code> { one-off</td>
<td>repeating } <code>start-time</code> <code>start-date</code> <code>end-time</code> <code>end-date</code> <code>offset-time</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute this command in user view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.</td>
</tr>
<tr>
<td>Enter system view from user view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Set the system name of the switch</td>
<td><code>sysname sysname</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Return from current view to lower level view</td>
<td><code>quit</code></td>
<td>By default, the name is 5500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the current view is user view, you will quit the current user interface.</td>
</tr>
<tr>
<td>Return from current view to user view</td>
<td><code>return</code></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The composite key &lt;Ctrl+Z&gt; has the same effect with the <code>return</code> command.</td>
</tr>
</tbody>
</table>
Displaying the System Status

You can use the following `display` commands to check the status and configuration information about the system. For information about protocols and ports, and the associated `display` commands, refer to relevant sections.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current date and time of the system</td>
<td><code>display clock</code></td>
<td>You can execute the <code>display</code> commands in any view</td>
</tr>
<tr>
<td>Display the version of the system</td>
<td><code>display version</code></td>
<td></td>
</tr>
<tr>
<td>Display the information about users logging onto the switch</td>
<td><code>display users [ all ]</code></td>
<td></td>
</tr>
</tbody>
</table>

Debugging the System

Enabling/Disabling System Debugging

The Ethernet switch provides a variety of debugging functions. Most of the protocols and features supported by the Ethernet switch are provided with corresponding debugging functions. These debugging functions help users diagnose and troubleshoot the system faults.

The output of debugging information is determined by the following two settings:

- Protocol debugging setting, which controls whether the debugging information of a protocol is output.
- Terminal display setting, which controls whether the debugging information is output to the screen of a specific user.

The relationship between the two settings is as follows:
You can use the following commands to enable the two settings.

### Table 691 Enable debugging and terminal display for a specific module

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable system debugging for specific module</td>
<td><code>debugging module-name [debugging-option]</code></td>
<td>Required&lt;br&gt;Disabled for all modules by default.</td>
</tr>
<tr>
<td>Enable terminal display for debugging</td>
<td><code>terminal debugging</code></td>
<td>Required&lt;br&gt;Disabled by default.</td>
</tr>
</tbody>
</table>

**CAUTION:** The output of debugging information affects the system operation. Disable all debugging after you finish the system debugging.

### Displaying Debugging Status

### Table 692 Display the current debugging status in the system

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display all enabled debugging on the specified device</td>
<td>`display debugging [fabric</td>
<td>unit unit-id] [interface</td>
</tr>
<tr>
<td>Display all enabled debugging in the Fabric by module</td>
<td><code>display debugging fabric by-module</code></td>
<td></td>
</tr>
</tbody>
</table>
When an Ethernet switch is in trouble, you may need to view a lot of operating information to locate the problem. Each functional module has its corresponding operating information display command(s). You can use the command here to display the current operating information about the modules in the system for troubleshooting your system.

**Table 693** Display the current operation information about the modules in the system.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current operation information about the modules in the system.</td>
<td><code>display diagnostic-information</code></td>
<td>You can use this command in any view. You should execute this command twice to find the difference between the two executing results, thus helping locate the problem.</td>
</tr>
</tbody>
</table>
Network Connectivity Test

You can use the **ping** command to check the network connectivity and the reachability of a host.

**Table 694 The ping command**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>

This command can output the following results:

- **Response status for each ping packet.** If no response packet is received within the timeout time, the message **Request time out** is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.

- **Final statistics,** including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

You can use the **tracert** command to trace the gateways that a packet passes from the source to the destination. This command is mainly used to check the network connectivity. It can also be used to help locate the network faults.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.
### Table 695  The tracert command

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the gateways that a packet passes from the source host to the destination</td>
<td><code>tracert [-a source-ip] [-f first-ttl] [-m max-ttl] [-p port] [-q num-packet] [-w timeout] string</code></td>
<td>You can execute the <code>tracert</code> command in any view.</td>
</tr>
</tbody>
</table>
Device Management

Introduction to Device Management

Device Management includes the following functions:

- Reboot the Ethernet switch
- Specify the application to be used at the next reboot
- Configure real-time monitoring of the running status of the system
- Update the Boot ROM
- Update the host software of the switches in the Fabric
- Identifying and Diagnosing Pluggable Transceivers

Device Management Configuration

Device Management Configuration Tasks

Table 696 Device management configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Rebooting the Ethernet Switch”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Scheduling a Reboot on the Switch”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Specifying the APP to be Used at Reboot”</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring Real-time Monitoring of the Running Status of the System”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Upgrading the Boot ROM”</td>
<td>Optional</td>
</tr>
<tr>
<td>“Upgrading the Host Software in the Fabric”</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Rebooting the Ethernet Switch

You can perform the following operation in user view when the switch is faulty or needs to be rebooted.

Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations.

Table 697 Reboot the Ethernet switch

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the Ethernet switch</td>
<td>reboot [ unit unit-id ]</td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.
The switch timer can be set to precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

### Specifying the APP to be Used at Reboot

APP is the host software of the switch. If multiple APPs exist in the Flash memory, you can use the command here to specify the one that will be used when the switch reboots.

#### Table 699 Specify the APP to be used at reboot

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the APP to be used at reboot</td>
<td>boot boot-loader [backup-attribute] {file-url [fabric]</td>
<td>device-name}</td>
</tr>
</tbody>
</table>

### Configuring Real-time Monitoring of the Running Status of the System

This function enables you to dynamically record the system running status, such as CPU, thus facilitating analysis and solution of the problems of the device.

#### Table 700 Configure real-time monitoring of the running status of the system

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable real-time monitoring of the running status of the system</td>
<td>system-monitor enable</td>
<td>Optional Enabled by default.</td>
</tr>
</tbody>
</table>

**CAUTION:** Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to release your CPU resources.

### Upgrading the Boot ROM

You can use the Boot ROM program saved in the Flash memory of the switch to upgrade the running Boot ROM. With this command, a remote user can conveniently upgrade the Boot Rom by uploading the Boot ROM to the switch through FTP and running this command. The Boot ROM can be used when the switch restarts.
Upgrading the Host Software in the Fabric

You can execute the following command on any device in a Fabric to use specified host software to upgrade all devices in a Fabric, thus realizing the software version consistency in this Fabric.

Table 701 Upgrade the Boot ROM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade the Boot ROM</td>
<td>`boot bootrom { file-url</td>
<td>device-name }`</td>
</tr>
</tbody>
</table>

Table 702 Upgrade the host software in the Fabric

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade the host software on the devices in the Fabric</td>
<td>`update fabric { file-url</td>
<td>device-name }`</td>
</tr>
</tbody>
</table>

Identifying and Diagnosing Pluggable Transceivers

Introduction to pluggable transceivers

Four types of pluggable transceivers are commonly used and can be divided into optical transceivers and electrical transceivers based on transmission media as shown in Table 703.

Table 703 Commonly used pluggable transceivers

<table>
<thead>
<tr>
<th>Transceiver type</th>
<th>Applied environment</th>
<th>Whether can be an optical transceiver</th>
<th>Whether can be an electrical transceiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP (Small Form-factor Pluggable)</td>
<td>Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GBIC (GigaBit Interface Converter)</td>
<td>Generally used for 1000M Ethernet interfaces</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>XFP (10-Gigabit small Form-factor Pluggable)</td>
<td>Generally used for 10G Ethernet interfaces</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>XENPAK (10 Gigabit EtherNet Transceiver Package)</td>
<td>Generally used for 10G Ethernet interfaces</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For pluggable transceivers supported by the Switche 5500, refer to Switch 5500 Family Getting Started Guide.

Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can perform the following configurations to identify main parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or vendor name specified.

Table 704 Identifying pluggable transceivers

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display main parameters of the pluggable transceiver(s)</td>
<td><code>display transceiver interface [ interface-type interface-number ]</code></td>
<td>Available for all pluggable transceivers</td>
</tr>
</tbody>
</table>
You can use the Vendor Name field in the prompt information of the display transceiver interface command to identify an anti-spoofing pluggable transceiver customized by 3Com. If the field is 3Com, it is considered an 3Com-customized pluggable transceiver.

Electrical label information is also called permanent configuration data or archive information, which is written to the storage device of a card during device debugging or test. The information includes name of the card, device serial number, and vendor name or vendor name specified.

**Diagnosing pluggable transceivers**

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. Optical transceivers customized by 3Com also support the digital diagnosis function, which enables a transceiver to monitor the main parameters 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.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current alarm information of the pluggable transceiver(s)</td>
<td><code>display transceiver alarm interface [ interface-type interface-number ]</code></td>
<td>Available for all pluggable transceivers</td>
</tr>
<tr>
<td>Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by 3Com</td>
<td><code>display transceiver diagnosis interface [ interface-type interface-number ]</code></td>
<td>Available for anti-spoofing pluggable optical transceiver(s) customized by 3Com only</td>
</tr>
</tbody>
</table>

**Displaying the Device Management Configuration**

After completing the above configuration, you can execute the `display` command in any view to display the operating status of the device management to verify the configuration effects.
Remote Switch APP Upgrade Configuration Example

Network requirements
Telnet to the switch from a PC remotely and download applications from the FTP server to the Flash memory of the switch. Update the switch software by using the device management commands through CLI.

The switch acts as the FTP client, and the remote PC serves as both the configuration PC and the FTP server.

Perform the following configuration on the FTP server.

- Configure an FTP user, whose name is switch and password is hello. Authorize the user with the read-write right on the directory Switch on the PC.
- Make configuration so that the IP address of a VLAN interface on the switch is 1.1.1.1, the IP address of the PC is 2.2.2.2, and the switch and the PC is reachable to each other.

The host software switch.bin and the Boot ROM file boot.btm of the switch are stored in the directory switch on the PC. Use FTP to download the switch.bin and boot.btm files from the FTP server to the switch.

Table 706 Display the operating status of the device management

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the APP to be adopted at next startup</td>
<td>display boot-loader [ unit unit-id ]</td>
<td>You can execute the display command in any view.</td>
</tr>
<tr>
<td>Display the module type and operating status of each board</td>
<td>display device [ manuinfo [ unit unit-id ]</td>
<td>unit unit-id ]</td>
</tr>
<tr>
<td>Display CPU usage of a switch</td>
<td>display cpu [ unit unit-id ]</td>
<td></td>
</tr>
<tr>
<td>Display the operating status of the fan</td>
<td>display fan [ unit unit-id [ fan-id ] ]</td>
<td></td>
</tr>
<tr>
<td>Display memory usage of a switch</td>
<td>display memory [ unit unit-id [ limit ]</td>
<td></td>
</tr>
<tr>
<td>Display the operating status of the power supply</td>
<td>display power [ unit unit-id [ power-id ] ]</td>
<td></td>
</tr>
<tr>
<td>Display system diagnostic information or save system diagnostic information to a file with the extension .diag into the Flash memory</td>
<td>display diagnostic-information</td>
<td></td>
</tr>
<tr>
<td>Display enabled debugging on a specified switch or all switches in the fabric</td>
<td>display debugging [ fabric</td>
<td>unit unit-id ] [ interface interface-type interface-number ] [ module-name ]</td>
</tr>
<tr>
<td>Display enabled debugging on all switches in the fabric by modules</td>
<td>display debugging fabric by-module</td>
<td></td>
</tr>
</tbody>
</table>
Network diagram

Figure 292  Network diagram for FTP configuration

![Network diagram](image)

Configuration procedure

1. Configure the following FTP server-related parameters on the PC: an FTP user with the username as switch and password as hello, who is authorized with the read-write right on the directory Switch on the PC. The detailed configuration is omitted here.

2. On the switch, configure a level 3 telnet user with the username as user and password as hello. Authentication mode is by user name and password.

   Refer to “Logging into an Ethernet Switch” on page 31 for configuration commands and steps about using telnet.

3. Execute the `telnet` command on the PC to log into the switch. The following prompt appears:

   `<5500>`

   **CAUTION:** If the Flash memory of the switch is not sufficient, delete the original applications before downloading the new ones.

4. Initiate an FTP connection with the following command in user view. Enter the correct user name and password to log into the FTP server.

   `<5500>` `ftp 2.2.2.2`
   Trying ...
   Press CTRL+K to abort
   Connected.
   220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
   User(none):switch
   331 Give me your password, please
   Password:*****
   230 Logged in successfully
   [ftp]

5. Enter the authorized path on the FTP server.

   `[ftp] cd switch`

6. Execute the `get` command to download the switch.bin and boot.btm files on the FTP server to the Flash memory of the switch.

   `[ftp] get switch.bin
   [ftp] get boot.btm`

7. Execute the `quit` command to terminate the FTP connection and return to user view.

   `[ftp] quit
   `<5500>`

8. Upgrade the Boot ROM.

   `<5500>` `boot bootrom boot.btm`
   This will update BootRom file on unit 1. Continue? [Y/N] y
Upgrading BOOTROM, please wait...
Upgrade BOOTROM succeeded!

9 Specify the downloaded program as the host software to be adopted when the switch starts next time.

```
<5500> boot boot-loader switch.bin
The specified file will be booted next time on unit 1!
```

```
<5500> display boot-loader
Unit 1:
  The current boot app is: switch.bin
  The main boot app is: switch.bin
  The backup boot app is:
```

# Reboot the switch to upgrade the Boot ROM and host software of the switch.

```
<5500> reboot
```
VLAN-VPN Overview

Introduction to VLAN-VPN

Virtual private network (VPN) is a new technology that emerges with the expansion of the Internet. It can be used for establishing private networks over the public network. With VPN, you can specify to process packets on the client or the access end of the service provider in specific ways, establish dedicated tunnels for user traffic on public network devices, and thus improve data security.

VLAN-VPN feature is a simple yet flexible Layer 2 tunneling technology. It tags private network packets with outer VLAN tags, thus enabling the packets to be transmitted through the service providers’ backbone networks with both inner and outer VLAN tags. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks), and the inner VLAN tags are treated as part of the payload.

Figure 293 describes the structure of the packets with single-layer VLAN tags.

Figure 293  Structure of packets with single-layer VLAN tags

Figure 294 describes the structure of the packets with double-layer VLAN tags.

Figure 294  Structure of packets with double-layer VLAN tags

Compared with MPLS-based Layer 2 VPN, VLAN-VPN has the following features:
It provides Layer 2 VPN tunnels that are simpler.

VLAN-VPN can be implemented through manual configuration. That is, signaling protocol-related configuration is not needed.

The VLAN-VPN feature provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

**Implementing VLAN-VPN**

With the VLAN-VPN feature enabled, no matter whether or not a received packet already carries a VLAN tag, the switch will tag the received packet with the default VLAN tag of the receiving port and add the source MAC address to the MAC address table of the default VLAN. When a packet reaches a VLAN-VPN-enabled port:

- If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet.
- Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

**Configuring the TPID for VLAN-VPN Packets**

This section applies to the Switch 5500 only, not the Switch 5500G.

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The value of this field is 0x8100 for IEEE 802.1Q. Figure 295 illustrates the structure of the IEEE 802.1Q VLAN tag in an Ethernet frame.

**Figure 295** The structure of the VLAN tag in an Ethernet frame

<table>
<thead>
<tr>
<th>0</th>
<th>15</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPID</td>
<td>Priority</td>
<td>VLAN ID</td>
</tr>
</tbody>
</table>

A Switch 5500 determines whether a received frame is VLAN tagged by comparing its own TPID with the TPID field in the received frame. If they match, the frame is considered as a VLAN tagged frame. If not, the switch tags the frame with the default VLAN tag of the receiving port.

By default, a Switch 5500 adopt the IEEE 802.1Q TPID value 0x8100. Some vendors, however, use other TPID values such as 0x9100. For compatibility with these systems, the Switch 5500 allows you to change the TPID that a port uses when tagging a received VLAN-VPN frame as needed. When doing that, you should set the same TPID on both the customer-side port and the service provider-side port.

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, you cannot set the TPID value to any of the values in the table below.
Inner-to-Outer Tag Priority Replicating and Mapping

As shown in Figure 295, the user priority field is the 802.1p priority of the tag. The value of this 3-bit field is in the range 0 to 7. By configuring inner-to-outer tag priority replicating or mapping for a VLAN-VPN-enabled port, you can replicate the inner tag priority to the outer tag or assign outer tags of different priorities to packets according to their inner tag priorities.

Refer to “QoS Profile Configuration” on page 710 for information about setting the priority.

Table 707  Commonly used protocol type values in Ethernet frames

<table>
<thead>
<tr>
<th>Protocol type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>0x0806</td>
</tr>
<tr>
<td>IP</td>
<td>0x0800</td>
</tr>
<tr>
<td>MPLS</td>
<td>0x8847/0x8848</td>
</tr>
<tr>
<td>IPX</td>
<td>0x8137</td>
</tr>
<tr>
<td>IS-IS</td>
<td>0x8000</td>
</tr>
<tr>
<td>LACP</td>
<td>0x8809</td>
</tr>
<tr>
<td>802.1x</td>
<td>0x888E</td>
</tr>
</tbody>
</table>

Table 708  VLAN-VPN configuration tasks

<table>
<thead>
<tr>
<th>Operation Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the VLAN-VPN feature for a port</td>
<td>“Enabling the VLAN-VPN Feature for a Port”</td>
</tr>
<tr>
<td>Adjust the TPID value for VLAN-VPN packets on a port</td>
<td>“Configuring the TPID Value for VLAN-VPN Packets on a Port”</td>
</tr>
<tr>
<td>Configure the inner-to-outer tag priority replicating and mapping feature</td>
<td>“Configuring the Inner-To-Outer Tag Priority Replicating and Mapping Feature”</td>
</tr>
</tbody>
</table>

**CAUTION:** As IRF fabric is mutually exclusive with VLAN-VPN, make sure that IRF fabric is disabled on the switch before performing any of the configurations listed in Table 708. For information about IRF fabric, refer to the section entitled “IRF Fabric Configuration” on page 733.

Enabling the VLAN-VPN Feature for a Port

Table 709  Enable the VLAN-VPN feature for a port

<table>
<thead>
<tr>
<th>Operation Description</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Enable the VLAN-VPN feature on the port</td>
<td>vlan-vpn enable</td>
<td>Required By default, the VLAN-VPN feature is disabled on a port.</td>
</tr>
</tbody>
</table>
CHAPTER 80: VLAN-VPN CONFIGURATION

Configuring the TPID Value for VLAN-VPN Packets on a Port

On the Switch 5500 (not the Switch 5500G), for your device to correctly identify the VLAN tagged frames from the public network, make sure that the TPID you will use is the same as that used on the peer device in the public network. Follow the instructions in Table 710.

Table 710  Configure the TPID value for VLAN-VPN packets on a port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Set the TPID value on the port</td>
<td><code>vlan-vpn tpid value</code></td>
<td>Required</td>
</tr>
</tbody>
</table>

- Besides the default TPID 0x8100, you can configure only one TPID value on a Switch 5500.
- For the Switch 5500 to exchange packets with the public network device properly, you should configure the TPID value used by the public network device on both the customer-side port and the service provider-side port.

Make sure that the VLAN-VPN feature is enabled on a port before configuring the inner-to-outer tag priority replicating and mapping feature.

Table 711  Configure the inner-to-outer tag priority replicating and mapping feature

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable the inner-to-outer tag priority replicating feature</td>
<td><code>vlan-vpn inner-cos-trust enable</code></td>
<td>Either of the two configurations is required.</td>
</tr>
<tr>
<td>Enable the inner-to-outer tag priority mapping feature and create a priority mapping</td>
<td><code>vlan-vpn priority old-priority remark new-priority</code></td>
<td>By default, neither the inner-to-outer tag priority replicating feature nor the inner-to-outer tag priority mapping feature is enabled.</td>
</tr>
</tbody>
</table>

CAUTION:

- If you have configured the port priority (refer to “QoS Profile Configuration” on page 709), you will be prompted that the port priority configured for the current port gets invalid after you enable the inner-to-outer tag priority replicating feature.
- The inner-to-outer tag priority replicating feature is mutually exclusive with the inner-to-outer tag priority mapping feature.
After the configuration above, you can execute the `display` command in any view to view the running status of VLAN-VPN and verify the configuration.

**Table 712**  Display VLAN-VPN configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the VLAN-VPN configurations of all the ports</td>
<td><code>display port vlan-vpn</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
</tbody>
</table>

**Network requirements**

As shown in Figure 296, Switch A and Switch B are both Switch 5500s. They connect the users to the servers through the public network.

- PC users and PC servers are in VLAN 100 created in the private network, while terminal users and terminal servers are in VLAN 200, which is also created in the private network. The VLAN VPN connection is established in VLAN 1040 of the public network.
- Switches of other vendors’ are used in the public network. They use the TPID value 0x9200.
- Employ VLAN-VPN on Switch A and Switch B to enable the PC users and PC servers to communicate with each through a VPN, and employ VLAN-VPN on Switch A and Switch B to enable the Terminal users and Terminal servers to communicate with each other through a VPN.
CHAPTER 80: VLAN-VPN CONFIGURATION

Network diagram

Figure 296  Network diagram for VLAN-VPN configuration

Switch 5500 Configuration procedure

Configure Switch A.

# Enable the VLAN-VPN feature on Ethernet 1/0/11 of Switch A and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchA> system-view
[SwitchA] vlan 1040
[SwitchA-vlan1040] port Ethernet 1/0/11
[SwitchA-vlan1040] quit
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] vlan-vpn enable
[SwitchA-Ethernet1/0/11] quit
```

# Set the TPID value of Ethernet 1/0/12 to 0x9200 (for intercommunication with the devices in the public network) and configure the port as a trunk port permitting packets of VLAN 1024.

```
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] vlan-vpn tpid 9200
[SwitchA-Ethernet1/0/12] port link-type trunk
[SwitchA-Ethernet1/0/12] port trunk permit vlan 1040
```

Configure Switch B.

# Enable the VLAN-VPN feature on Ethernet 1/0/21 of Switch B and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
```
VLAN-VPN Configuration Example

949

<SwitchB> system-view
[SwitchB] vlan 1040
[SwitchB-vlan1040] port Ethernet 1/0/21
[SwitchB-vlan1040] quit
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/21] vlan-vpn enable

Set the TPID value of Ethernet1/0/21 to 0x9200 (for intercommunication with the devices in the public network) and set the port as a trunk port permitting packets of VLAN 1024.

[SwitchB-Ethernet1/0/22] vlan-vpn tpid 9200
[SwitchB-Ethernet1/0/22] quit
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/22] port link-type trunk
[SwitchB-Ethernet1/0/22] port trunk permit vlan 1040

- Do not configure VLAN 1040 as the default VLAN of Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B. Otherwise, the outer VLAN tag of a packet will be removed during transmission.

- In this example, both Ethernet1/0/11 of Switch A and Ethernet1/0/21 of Switch B are access ports. In cases where the ports are trunk ports or hybrid ports, you need to configure the two ports to remove the outer VLAN tags before transmitting packets of VLAN 1040. Refer to “Port Basic Configuration” on page 159 for detailed configuration instructions.

- Configure the devices in the public network

# As the devices in the public network are from other vendors, only the basic principles are introduced here. That is, you need to configure the devices connecting to Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B to permit the corresponding ports to transmit tagged packets of VLAN 1040.

Switch 5500G Configuration Procedure

- Configure Switch A.

# Enable the VLAN-VPN feature on GigabitEthernet 1/0/11 of Switch A and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

<SwitchA> system-view
[SwitchA] vlan 1040
[SwitchA-vlan1040] port GigabitEthernet 1/0/11
[SwitchA-vlan1040] quit
[SwitchA] interface GigabitEthernet 1/0/11
[SwitchA-GigabitEthernet1/0/11] vlan-vpn enable
[SwitchA-GigabitEthernet1/0/11] quit

# Configure GigabitEthernet 1/0/12 as a trunk port permitting packets of VLAN 1040.

[SwitchA] interface GigabitEthernet 1/0/12
[SwitchA-GigabitEthernet1/0/12] port link-type trunk
[SwitchA-GigabitEthernet1/0/12] port trunk permit vlan 1040

- Configure Switch B.

# Enable the VLAN-VPN feature on GigabitEthernet 1/0/21 of Switch B and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.
Do not configure VLAN 1040 as the default VLAN of GigabitEthernet 1/0/12 of Switch A and GigabitEthernet 1/0/22 of Switch B. Otherwise, the outer VLAN tag of a packet will be removed during transmission.

In this example, both GigabitEthernet1/0/11 of Switch A and GigabitEthernet1/0/21 of Switch B are access ports. In cases where the ports are trunk ports or hybrid ports, you need to configure the two ports to remove the outer VLAN tags before transmitting packets of VLAN 1040. Refer to VLAN Configuration in this manual for detailed configuration.

Configure the devices in the public network
# As the devices in the public network are from other vendors, only the basic principles are introduced here. That is, you need to configure the devices connecting to GigabitEthernet 1/0/12 of Switch A and GigabitEthernet 1/0/22 of Switch B to permit the corresponding ports to transmit tagged packets of VLAN 1040.

Data transfer process
The following describes how a packet is forwarded from Switch A to Switch B in this example.

1 As Ethernet 1/0/11 of Switch A is a VLAN-VPN port, when a packet from the customer's network side reaches this port, it is tagged with the default VLAN tag of the port (VLAN 1040).

2 The TPID value of the outer VLAN tag is set to 0x9200 before the packet is forwarded to the public network through Ethernet1/0/12 of Switch A.

3 The outer VLAN tag of the packet remains unchanged while the packet travels in the public network, till it reaches Ethernet1/0/22 of Switch B.

4 After the packet reaches Switch B, it is forwarded through Ethernet1/0/21 of Switch B. As the port belongs to VLAN 1040 and is an access port, the outer VLAN tag (the tag of VLAN 1040) of the packet is removed before the packet is forwarded, which restores the packet to a packet tagged with only the private VLAN tag and enables it to be forwarded to its destination networks.

5 It is the same case when a packet travels from Switch B to Switch A.
Selective QinQ Overview

Selective QinQ is an enhanced application of the VLAN-VPN feature. With the selective QinQ feature, you can configure inner-to-outer VLAN tag mapping, according to which you can add different outer VLAN tags to the packets with different inner VLAN tags.

The selective QinQ feature makes the service provider network structure more flexible. You can classify the terminal users on the port connecting to the access layer device according to their VLAN tags, and add different outer VLAN tags to these users. In the public network, you can configure QoS policies based on outer VLAN tags to assign different priorities to different packets, thus providing differentiated services. See Figure 297 for details.

Figure 297  Diagram for a selective QinQ implementation

In this implementation, Switch A is an access device of the service provider. The users connecting to it include common customers (in VLAN 8 to VLAN 100), VIPs (in VLAN 101 to VLAN 200), and IP telephone users (in VLAN 201 to VLAN 300). Packets of all these users are forwarded by Switch A to the public network.
After the selective QinQ feature and the inner-to-outer tag mapping feature are enabled on the port connecting Switch A to these users, the port will add different outer VLAN tags to the packets according to their inner VLAN tags. For example, you can configure to add the tag of VLAN 1002 to the packets of IP telephone users in VLAN 201 to VLAN 300 and forward the packets to the VoIP device, which is responsible for processing IP telephone services.

To guarantee the quality of voice packet transmission, you can configure QoS policies in the public network to reserve bandwidth for packets of VLAN 1002 and forward them preferentially.

In this way, you can configure different forwarding policies for data of different type of users, thus improving the flexibility of network management. On the other hand, network resources are well utilized, and users of the same type are also isolated by their inner VLAN tags. This helps to improve network security.

**MAC Address Replicating**

Like the VLAN-VPN feature, a port with the selective QinQ enabled adds the source MAC addresses of user packets to the MAC address table of the default VLAN on the port. However, the port with selective QinQ enabled can insert an outer VLAN tag other than that of the default VLAN to the packets. Thus, when packets are forwarded from the service provider to users, they may be broadcast if their destination MAC addresses cannot be found in the MAC address table of the outer VLANs.

As shown in Figure 298, the default VLAN of the port used to receive packets is VLAN 2. The port is configured to receive packets of VLAN 3, tag the received packets with the outer tag of VLAN 4, and add the source MAC addresses (MAC-A) of the packets to the MAC address table of its default VLAN (VLAN 2).

When a response packet is returned to the device from VLAN 4 of the service provider network, the device searches the outbound port for MAC-A in the MAC
address table of VLAN 4. However, because the corresponding entry is not added
the MAC address table of VLAN 4, this packet is considered to be a unicast
packet with unknown destination MAC address. As a result, this packet will be
broadcast to all the ports in VLAN 4, which wastes the network resources and
incurs potential security risks.

The Switch 5500 provides the inter-VLAN MAC address replicating feature, which
can replicate the entries in the MAC address table of the default VLAN to that of
the VLAN corresponding to the outer tag. With the inter-VLAN MAC address
replicating feature enabled, when a device receives a packet from the service
provider network, this device will find the path for the packet by searching the
MAC address table of the VLAN corresponding to the outer tag and unicast the
packet. Thus, packet broadcast is reduced in selective QinQ applications.

Likewise, the entries in the MAC address table of the outer VLAN can also be
replicated to that of the default VLAN on a port, through which the outbound
port to the service provider network can be determined through the MAC address
table of the default VLAN and user packets destined for the service provider can
be unicast.

### Selective QinQ Configuration

<table>
<thead>
<tr>
<th>Selective QinQ Configuration Tasks</th>
<th>Operation</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selective QinQ feature for a port</td>
<td>Required</td>
<td>“Enabling the Selective QinQ Feature for a Port”</td>
<td></td>
</tr>
<tr>
<td>Enable the inter-VLAN MAC address replicating feature</td>
<td>Optional</td>
<td>“Enabling the Inter-VLAN MAC Address Replicating Feature”</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:** If IRF Fabric has been enabled on a device, you cannot enable the VLAN-VPN feature and the selective QinQ feature on any port of the device.

### Enabling the Selective QinQ Feature for a Port

The following configurations are required for the selective QinQ feature:

- Enabling the VLAN-VPN feature on the current port
- Configuring the current port to permit packets of specific VLANs (the VLANs whose tags are to be used as the outer VLAN tags are required)

**Table 713** Enable the selective QinQ feature

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure the outer VLAN tag and enter QinQ view</td>
<td>vlan-vpn vid vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td>Configure to add outer VLAN tags to the packets with the specific inner VLAN tags</td>
<td>raw-vlan-id inbound vlan-id-list</td>
<td>Required</td>
</tr>
</tbody>
</table>

By default, the feature of adding an outer VLAN tag to the packets with the specific inner VLAN tags is disabled.
Do not enable both the selective QinQ function and the DHCP snooping function on a switch. Otherwise, the DHCP snooping function may operate improperly.

**Enabling the Inter-VLAN MAC Address Replicating Feature**

Table 714 Enable the inter-VLAN MAC address replicating feature

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable the inter-VLAN MAC address replicating feature</td>
<td><code>mac-address-mapping</code></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td><code>index</code></td>
<td>By default, the inter-VLAN MAC address replicating feature is disabled.</td>
</tr>
<tr>
<td></td>
<td><code>source-vlan</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>source-vlan-id-list</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>destination-vlan</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>dest-vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:**
- On a port, the inter-VLAN MAC address replicating feature can be configured only once for a destination VLAN. If the configuration needs to be modified, you need to remove the existing configuration first.
- With the inter-VLAN MAC address replicating feature disabled, all the MAC address entries that the destination VLAN learns from the other VLANs through this function are removed.
- MAC address entries obtained through the inter-VLAN MAC address replicating feature cannot be removed manually. To remove a MAC address entry of this kind, you need to disable the inter-VLAN MAC address replicating feature first.
- VLAN 4093 is a special VLAN reserved for the IRF fabric feature. It cannot serve as the destination VLAN of the inter-VLAN MAC address replicating feature to receive MAC address entries from the other VLANs.

**Selective QinQ Configuration Example**

**Processing Private Network Packets by Their Types**

**Network requirements**
- Ethernet 1/0/3 of Switch A provides public network access for PC users and IP phone users. PC users belong to VLAN 100 through VLAN 108, and IP phone users belong to VLAN 200 through VLAN 230. Ethernet 1/0/5 of Switch A is connected to the public network. The peer end of Switch A is Switch B.
- Ethernet 1/0/11 of Switch B is connected to the public network. Ethernet 1/0/12 and Ethernet 1/0/13 of Switch B provide network access for PC servers belonging to VLAN 100 through VLAN 108 and voice gateways (for IP phone users) belonging to VLAN 200 through VLAN 230 respectively.
- The public network permits packets of VLAN 1000 and VLAN 1200. Apply QoS policies for these packets to reserve bandwidth for packets of VLAN 1200. That is, packets of VLAN 1200 have higher transmission priority over packets of VLAN 1000.
- Employ the selective QinQ feature on Switch A and Switch B to differentiate traffic of PC users from that of IP phone users, for the purpose of using QoS policies to guarantee higher priority for voice traffic.
To reduce broadcast packets in the network, enable the inter-VLAN MAC address replicating feature for selective QinQ.

**Network diagram**

*Figure 299  Network diagram for selective QinQ configuration*

![Network diagram](image)

**Configuration procedure**

- Configure Switch A.

  # Create VLAN 1000, VLAN 1200 and VLAN 5 (the default VLAN of Ethernet 1/0/3) on SwitchA.

  ```
  <SwitchA> system-view
  [SwitchA] vlan 1000
  [SwitchA-vlan1000] quit
  [SwitchA] vlan 1200
  [SwitchA-vlan1200] quit
  [SwitchA] vlan 5
  [SwitchA-vlan5] quit
  ```

  **Table 715  # Configure Ethernet 1/0/5 as a hybrid port and configure VLAN 5 as its default VLAN. Configure Ethernet 1/0/5 not to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.**

  ```
  [SwitchA] interface Ethernet 1/0/5
  [SwitchA-Ethernet1/0/5] port link-type hybrid
  [SwitchA-Ethernet1/0/5] port hybrid pvid vlan 5
  [SwitchA-Ethernet1/0/5] port hybrid vlan 5 1000 1200 tagged
  [SwitchA-Ethernet1/0/5] quit
  ```

  # Configure Ethernet 1/0/3 as a hybrid port and configure Ethernet1/0/3 to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.
CHAPTER 81: SELECTIVE QINQ CONFIGURATION

[SwitchA] interface Ethernet 1/0/3
[SwitchA-Etherent1/0/3] port link-type hybrid
[SwitchA-Etherent1/0/3] port hybrid vlan 5 1000 1200 untagged

# Enable the VLAN-VPN feature on Ethernet 1/0/3.

[SwitchA-Etherent1/0/3] vlan-vpn enable

# Enable the selective QinQ feature on Ethernet 1/0/3 to tag packets of VLAN 100 through VLAN 108 with the tag of VLAN 1000 as the outer VLAN tag, and tag packets of VLAN 200 through VLAN 230 with the tag of VLAN 1200 as the outer VLAN tag.

[SwitchA-Etherent1/0/3] vlan-vpn vid 1000
[SwitchA-Etherent1/0/3-vid-1000] raw-vlan-id inbound 100 to 108
[SwitchA-Etherent1/0/3-vid-1000] quit
[SwitchA-Etherent1/0/3] vlan-vpn vid 1200
[SwitchA-Etherent1/0/3-vid-1200] raw-vlan-id inbound 200 to 230

# Enable the inter-VLAN MAC address replicating feature to replicate the MAC address entries of the MAC address tables of the outer VLANs to the MAC address table of the default VLAN, and replicate the MAC address entries of the MAC address table of the default VLAN to the MAC address tables of the outer VLANs.

[SwitchA-Etherent1/0/3-vid-1200] quit
[SwitchA-Etherent1/0/3] mac-address mapping 0 source-vlan 5 destination-vlan 1000
[SwitchA-Etherent1/0/3] mac-address mapping 1 source-vlan 5 destination-vlan 1200
[SwitchA-Etherent1/0/3] quit
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Etherent1/0/5] mac-address mapping 0 source-vlan 1000 1200 destination-vlan 5

After completing the above configuration, packets of VLAN 100 through VLAN 108 (that is, packets of PC users) are tagged with the tag of VLAN 1000 as the outer VLAN tag when they are forwarded to the public network by Switch A; and packets of VLAN 200 through VLAN 230 (that is, packets of IP phone users) are tagged with the tag of VLAN 1200 as the outer VLAN tag when they are forwarded to the public network.

■ Configure Switch B.

# Create VLAN 1000, VLAN 1200, VLAN 12 (the default VLAN of Ethernet1/0/12) and VLAN 13 (the default VLAN of Ethernet1/0/13) on Switch B.

<SwitchB> system-view
[SwitchB] vlan 1000
[SwitchB-vlan1000] quit
[SwitchB] vlan 1200
[SwitchB-vlan1200] quit
[SwitchB] vlan 12 to 13

# Configure Ethernet 1/0/11 as a hybrid port, and configure Ethernet 1/0/11 not to remove VLAN tags when forwarding packets of VLAN 12, VLAN 13, VLAN 1000, and VLAN 1200.
<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/11
[SwitchB-Etherent1/0/11] port link-type hybrid
[SwitchB-Etherent1/0/11] port hybrid vlan 12 13 1000 1200 tagged

# Configure Ethernet 1/0/12 as a hybrid port and configure VLAN 12 as its default VLAN. Configure Ethernet 1/0/12 to remove VLAN tags when forwarding packets of VLAN 12 and VLAN 1000.

[SwitchB] interface Ethernet 1/0/12
[SwitchB-Etherent1/0/12] port link-type hybrid
[SwitchB-Etherent1/0/12] port hybrid pvid vlan 12
[SwitchB-Etherent1/0/12] port hybrid vlan 12 1000 untagged
[SwitchB-Etherent1/0/12] quit

# Configure Ethernet 1/0/13 as a hybrid port and configure VLAN 13 as its default VLAN. Configure Ethernet 1/0/13 to remove VLAN tags when forwarding packets of VLAN 13 and VLAN 1200.

[SwitchB] interface Ethernet 1/0/13
[SwitchB-Etherent1/0/13] port link-type hybrid
[SwitchB-Etherent1/0/13] port hybrid pvid vlan 13
[SwitchB-Etherent1/0/13] port hybrid vlan 13 1200 untagged

After completing the above configuration, Switch B can forward packets of VLAN 1000 and VLAN 1200 to the corresponding servers through Ethernet 1/0/12 and Ethernet 1/0/13 respectively.

To make the packets from the servers be transmitted to the clients in the same way, you need to configure the selective QinQ feature and the inter-VLAN MAC address replicating feature on Ethernet 1/0/12 and Ethernet 1/0/13. The configuration on Switch B is similar to that on Switch A and is thus omitted.

- A selective QinQ-enabled device tags a user packet with an outer VLAN tag regardless of the VLAN tag of the user packet, so there is no need to configure user VLANs on the device.
- Make sure the packets of the default VLAN of a selective QinQ-enabled port are permitted on both the local port and the port connecting to the public network.
BPDU TUNNEL CONFIGURATION

BPDU Tunnel Overview

Introduction to the BPDU Tunnel Feature

Normally, Layer 2 protocols are needed in a LAN for network topology maintenance and management. For example, spanning tree protocol (STP) is used for maintaining spanning trees and preventing loops. 3Com group management protocol (Switch Clustering) is used for managing network topology and devices in a network.

When multiple branch networks of an organization are connected together through a public network, you can combine the corresponding network nodes into one so as to maintain the branch networks as a whole. This requires the packets of some of the user’s Layer 2 protocol packets be transmitted across the provider's network without getting involved in the computation of the public network.

The BPDU tunnel feature is designed to address the above requirements. It enables some Layer 2 protocol packets of private networks to be transmitted along tunnels established in the public network.

BPDU Tunnel Fundamental

Layer 2 protocol packet identification

Different from the processing of data packets, a Layer 2 protocol packet is classified first when it reaches a network device. A Layer 2 protocol packet conforming to IEEE standards carries a special destination MAC address (for example, the destination MAC address of an STP protocol packet is 0180-c200-0000) and contains a type field. Some proprietary protocols adopt the same packet structure, where a private MAC address is used to identify the corresponding proprietary protocol, and the type field is used to identify the specific protocol type.

Transmitting BPDU packets transparently

As shown in Figure 300, the network on the top is the service provider network, and the one on the bottom is a customer network. The service provider network contains edge devices connecting the customer network to the service provider network. The customer network contains Network A and Network B. You can make the BPDU packets of the customer network to be transmitted in the service provider network transparently by enabling the BPDU tunnel feature on the edge devices at both ends of the service provider network.
When a BPDU packet coming from a customer network reaches an edge device in the service provider network, the edge device changes the destination MAC address carried in the packet from a protocol-specific MAC address to a private multicast MAC address, which can be defined using a command. A packet with this multicast address as its destination address is called a tunnel packet. In the service provider network, the tunnel packet can be forwarded as a normal data packet.

Before the device in the service provider network forwards the packet to the destination customer network, the edge device will identify the tunnel packet, determine the packet type based on the type field in the packet, restore its destination MAC address to the original protocol-specific MAC address and then forward the packet to the access device on the user side. This ensures the packet to be forwarded is consistent with the packet before entering the tunnel. So, a tunnel here acts as a local link for user devices. It enables Layer 2 protocols to run on a virtual local network.

Figure 301 and Figure 302 show the structure of a BPDU packet before and after it enter a BPDU tunnel.

**Figure 300** BPDU Tunnel network hierarchy

![BPDU Tunnel network hierarchy](image)

**Figure 301** The structure of a BPDU packet before it enters a BPDU tunnel

<table>
<thead>
<tr>
<th>0</th>
<th>15</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC address (Specified by protocol)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BPDU Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You can establish BPDU tunnels between the Switch 5500 for the packets of the following protocols:

- LACP (link aggregation control protocol)
- STP (spanning tree protocol)
- Switch Clustering-related protocols, including: NDP (neighbor discovery protocol), NTDP (neighbor topology discovery protocol), cluster MRC (cluster member remote control), and HABP (3Com authentication bypass protocol)
- Proprietary protocols of other vendors, including CDP (CISCO discovery protocol), PAGP (port aggregation protocol), PVST (per-VLAN spanning tree), VTP (VLAN trunk protocol), and UDLD (uni-destinational link discovery)

**BPDU Tunnel Configuration**

**Configuration Prerequisites**

The edge devices can communicate with the user devices properly.

**Configuring a BPDU Tunnel**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure a private multicast MAC address for packets transmitted along the tunnel</td>
<td><code>bpdu-tunnel tunnel-dmac mac-address</code></td>
<td>Optional By default, the destination MAC address for packets transmitted along a BPDU tunnel is 010f-e200-0003.</td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Enable BPDU tunnel for packets of a specific protocol</td>
<td><code>bpdu-tunnel protocol-type</code></td>
<td>Required By default, BPDU tunnel is disabled for packets of any protocol.</td>
</tr>
</tbody>
</table>

- The BPDU Tunnel is unavailable to all the ports of a device if the device has the fabric feature enabled on one of its ports.
If BPDU tunnel transparent transmission is enabled for packets of a protocol, the protocol cannot be enabled on the port. For example, if you execute the `bpdu-tunnel lACP` command, the `lacp enable` command cannot be executed on the port.

The `bpdu-tunnel stp` command is mutually exclusive with the `vlan-vpn tunnel` command. Refer to “MSTP Configuration” on page 227 for details.

To enable BPDU tunnel transmission for PAGP packets, LACP packets and UDLD packets, make sure that the links the service provider provides are point-to-point links. Otherwise, these protocols cannot operate properly.

Because the NDP configuration and NTDP configuration cannot be synchronized to ports in an aggregation group, make sure that NDP and NTDP are not enabled on any port in an aggregation group before enabling the service provider network to use aggregation group to transmit Switch Clustering packets through BPDU tunnels.

The `bpdu-tunnel cdp` command is mutually exclusive with the `voice vlan legacy` command. Refer to “VLAN Configuration” on page 113 for details.

If a BPDU-tunnel-enabled port receives a tunnel packet from the customer’s network, errors occur in the network and the tunnel packet will be dropped directly.

---

**Displaying BPDU Tunnel Configuration**

After the configuration above, you can execute the `display` command in any view to view the private multicast address for tunnel packets and verify the configuration.

**Table 717** Display BPDU tunnel

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the private multicast MAC address used by the tunnel packets</td>
<td><code>display bpdu-tunnel</code></td>
<td>You can execute the <code>display</code> command in any view.</td>
</tr>
</tbody>
</table>

**BPDU Tunnel Configuration Example**

**Transmitting STP Packets Through a Tunnel**

- Customer1 and Customer2 are devices operating in a customer network; Provider1 and Provider2 are edge devices operating in the service provider network. The two devices receive data from the customer network by using Ethernet1/0/1 and Ethernet1/0/2 respectively.

- Provider1 and Provider2 are connected through trunk links, which permit packets of all VLANs.

- Enable the service provider network to transmit STP packets of the customer network through BPDU tunnel. The destination MAC address for tunnel packets is 010f-e233-8b22.

- Enable the VLAN-VPN feature for the service provider network, and enable the service provider network to use VLAN 100 to transmit data packets of the customer network.
Network diagram

Figure 303  Network diagram for BPDU Tunnel configuration

Configuration procedure

1  Configure Provider1.

# Disable STP on Ethernet1/0/1.

<5500> system-view
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] stp disable

# Enable the BPDU tunnel feature for STP BPDUs on Ethernet1/0/1.

[5500-Ethernet1/0/1] bpdu-tunnel stp

# Enable the VLAN-VPN feature on Ethernet1/0/1 and use VLAN 100 to transmit user data packets through BPDU tunnels.

[5500-Ethernet1/0/1] port access vlan 100
[5500-Ethernet1/0/1] vlan-vpn enable

# Configure the destination MAC address for protocol packets transmitted through the BPDU tunnel.

[5500-Ethernet1/0/1] quit
[5500] bpdu-tunnel tunnel-dmac 010f-e233-8b22

# Configure Ethernet1/0/2 as a trunk port that permits packets of all VLANs.

[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] port link-type trunk
[5500-Ethernet1/0/2] port trunk permit vlan all

2  Configure Provider2.

# Disable STP on Ethernet1/0/4.

<5500> system-view
[5500] interface Ethernet 1/0/4
[5500-Ethernet1/0/4] stp disable

# Enable BPDU tunnel for STP packets.
[5500-Ethernet1/0/4] bpdu-tunnel stp

# Enable VLAN-VPN and use VLAN 100 to transmit user data packets through BPDU tunnels.
[5500-Ethernet1/0/4] port access vlan 100
[5500-Ethernet1/0/4] vlan-vpn enable

# Configure the destination MAC address for the packets transmitted in the tunnel.
[5500-Ethernet1/0/4] quit
[5500] bpdu-tunnel tunnel-dmac 010f-e233-8b22

# Configure Ethernet1/0/3 as a trunk port that permits packets of all VLANs.
[5500] interface Ethernet 1/0/3
[5500-Ethernet1/0/3] port link-type trunk
[5500-Ethernet1/0/3] port trunk permit vlan all
Remote-ping is a network diagnostic tool. It is used to test the performance of various protocols running in networks. Remote-ping provides more functions than the ping command.

- The ping command can only use the ICMP protocol to test the round trip time (RTT) between this end and a specified destination end for the user to judge whether the destination end is reachable.

- Besides the above function of the ping command, remote-ping can also provide other functions, such as testing the status (open/close) of a DHCP/FTP/HTTP/SNMP server and the response time of various services.

You need to configure the remote-ping client and sometimes the corresponding remote-ping servers to perform various remote-ping tests. All remote-ping tests are initiated by the remote-ping client and you can view the test results on remote-ping client only.

When performing a remote-ping test, you need to configure a remote-ping test group on the remote-ping client. A remote-ping test group is a set of remote-ping test parameters. A test group contains several test parameters and is uniquely identified by an administrator name and a test tag.

After creating a remote-ping test group and configuring the test parameters, you can then perform a remote-ping test by the test-enable command.

- Being different from the ping command, remote-ping does not display the RTT or timeout status of each packet on the Console terminal in real time. To view the statistic results of your remote-ping test operation, you need to execute the display remote-ping command.

- Remote-ping also allows you to set parameters for remote-ping test groups, start remote-ping tests and view statistical test results through a network management device.

Figure 304  Remote-ping illustration
Among the test types supported by remote-ping, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled.

### Table 718  Test types supported by remote-ping

<table>
<thead>
<tr>
<th>Supported test types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP test</td>
<td>For these types of tests, you need to configure the remote-ping client and the corresponding servers.</td>
</tr>
<tr>
<td>DHCP test</td>
<td>■ These types of tests need the cooperation of the remote-ping client and remote-ping server.</td>
</tr>
<tr>
<td>FTP test</td>
<td>■ Do not perform a TCP, UDP or jitter test on a well-known port (ports with a number ranging from 1 to 1023) or on a port with a port number greater than 50000. Otherwise, your remote-ping test may fail or the service corresponding to the well-known port may become unavailable.</td>
</tr>
<tr>
<td>HTTP test</td>
<td></td>
</tr>
<tr>
<td>DNS test</td>
<td></td>
</tr>
<tr>
<td>SNMP test</td>
<td></td>
</tr>
<tr>
<td>Jitter test</td>
<td></td>
</tr>
<tr>
<td>TCP test</td>
<td>Tcppublic test</td>
</tr>
<tr>
<td></td>
<td>Tcpprivate test</td>
</tr>
<tr>
<td>UDP test</td>
<td>Udppublic test</td>
</tr>
<tr>
<td></td>
<td>Udpprivate test</td>
</tr>
</tbody>
</table>

### Remote-ping Test Parameters

You need to configure corresponding test parameters for each type of remote-ping test. remote-ping test parameters can be configured on remote-ping client only. For the configurations on remote-ping client, refer to “Remote-ping Client Configuration” on page 969.

### Table 719  Remote-ping test parameters

<table>
<thead>
<tr>
<th>Test parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination address (destination-ip)</td>
<td>For TCP/UDP/jitter test, you must specify a destination IP address, and the destination address must be the IP address of a TCP/UDP/UDP listening service configured on the remote-ping server.</td>
</tr>
<tr>
<td>Destination port (destination-port)</td>
<td>For tcpprivate/udpprivate/jitter test, you must specify a destination port number, and the destination port number must be the port number of a TCP or UDP listening service configured on the remote-ping server.</td>
</tr>
<tr>
<td>Source interface (source-interface)</td>
<td>■ For DHCP test, you must specify a source interface, which will be used by remote-ping client to send DHCP requests. If no source interface is specified for a DHCP test, the test will not succeed.</td>
</tr>
<tr>
<td></td>
<td>■ After a source interface is specified, remote-ping client uses this source interface to send DHCP requests during a DHCP test.</td>
</tr>
<tr>
<td></td>
<td>■ The IP address of the specified source interface will be used as the source IP address of DHCP requests.</td>
</tr>
</tbody>
</table>
### Remote-ping Overview

Source address (source-ip)

For remote-ping tests other than DHCP test, you can specify a source IP address for test packets, which will be used by the server as the destination address of response packets.

Source port (source-port)

For remote-ping tests other than ICMP, DHCP and DNS, you can specify a source port number for test packets, which will be used by the server as the destination port number of response packets.

Test type (test-type)

- You can use remote-ping to test a variety of protocols, see Table 718 for details.
- To perform a type of test, you must first create a test group of this type. One test group can be of only one remote-ping test type.
- If you modify the test type of a test group using the test-type command, the parameter settings, test results, and history records of the original test type are all cleared.

Number of probes per test (count)

- For tests except jitter test, only one test packet is sent in a probe. In a jitter test, you can use the jitter-packetnum command to set the number of packets to be sent in a probe.

Packet size (datasize)

- For ICMP/UDP/jitter test, you can configure the size of test packets.
- For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers).

Maximum number of history records that can be saved (history-records)

This parameter is used to specify the maximum number of history records that can be saved in a test group. When the number of saved history records exceeds the maximum number, remote-ping discards some earliest records.

Automatic test interval (frequency)

This parameter is used to set the interval at which the remote-ping client periodically performs the same test automatically.

Probe timeout time (timeout)

- The probe timeout timer is started after the remote-ping client sends out a test packet.
- This parameter is in seconds.

Type of service (tos)

Type of service is the value of the ToS field in IP header in the test packets.

dns

This parameter is used to specify a DNS domain name in a remote-ping DNS test group.

dns-server

This parameter is used to set the DNS server IP address in a remote-ping DNS test group.

HTTP operation type (http-operation)

This parameter is used to set the type of HTTP interaction operation between remote-ping client and HTTP server.

---

**Table 719** Remote-ping test parameters

<table>
<thead>
<tr>
<th>Test parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address (source-ip)</td>
<td>For remote-ping tests other than DHCP test, you can specify a source IP address for test packets, which will be used by the server as the destination address of response packets.</td>
</tr>
<tr>
<td>Source port (source-port)</td>
<td>For remote-ping tests other than ICMP, DHCP and DNS, you can specify a source port number for test packets, which will be used by the server as the destination port number of response packets.</td>
</tr>
</tbody>
</table>
| Test type (test-type)          | - You can use remote-ping to test a variety of protocols, see Table 718 for details.  
                                  - To perform a type of test, you must first create a test group of this type. One test group can be of only one remote-ping test type.  
                                  - If you modify the test type of a test group using the test-type command, the parameter settings, test results, and history records of the original test type are all cleared. |
| Number of probes per test (count) | - For tests except jitter test, only one test packet is sent in a probe. In a jitter test, you can use the jitter-packetnum command to set the number of packets to be sent in a probe. |
| Packet size (datasize)         | - For ICMP/UDP/jitter test, you can configure the size of test packets.  
                                  - For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers). |
| Maximum number of history records that can be saved (history-records) | This parameter is used to specify the maximum number of history records that can be saved in a test group. When the number of saved history records exceeds the maximum number, remote-ping discards some earliest records. |
| Automatic test interval (frequency) | This parameter is used to set the interval at which the remote-ping client periodically performs the same test automatically. |
| Probe timeout time (timeout)   | - The probe timeout timer is started after the remote-ping client sends out a test packet.  
                                  - This parameter is in seconds. |
| Type of service (tos)          | Type of service is the value of the ToS field in IP header in the test packets. |
| dns                            | This parameter is used to specify a DNS domain name in a remote-ping DNS test group. |
| dns-server                     | This parameter is used to set the DNS server IP address in a remote-ping DNS test group. |
| HTTP operation type (http-operation) | This parameter is used to set the type of HTTP interaction operation between remote-ping client and HTTP server. |
Remote-ping Configuration

The TCP/UDP/jitter tests need the cooperation of remote-ping client and remote-ping server. Other types of tests need to configure remote-ping client and corresponding different servers.

Configuration on a Remote-ping Server

You can enable both the remote-ping client and remote-ping server functions on a Switch 5500, that is, the switch can serve as a remote-ping client and server simultaneously.

### Table 719 Remote-ping test parameters

<table>
<thead>
<tr>
<th>Test parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP operation string and version (<strong>http-string</strong>)</td>
<td>This parameter is used to set the HTTP operation string and version in an HTTP test.</td>
</tr>
<tr>
<td>FTP operation type (<strong>ftp-operation</strong>)</td>
<td>This parameter is used to set the type of FTP interaction operation between remote-ping client and FTP server.</td>
</tr>
<tr>
<td>FTP operation type (<strong>ftp-operation</strong>)</td>
<td>This parameter is used to set the type of FTP interaction operation between remote-ping client and FTP server.</td>
</tr>
<tr>
<td>FTP login username and password (<strong>username</strong> and <strong>password</strong>)</td>
<td>The two parameters are used to set the username and password to be used for FTP operation.</td>
</tr>
<tr>
<td>File name for FTP operation (<strong>filename</strong>)</td>
<td>Name of a file to be transferred between remote-ping client and FTP server.</td>
</tr>
</tbody>
</table>
| Number of jitter test packets to be sent per probe (**jitter-packetnum**) | □ Jitter test is used to collect statistics about delay jitter in UDP packet transmission  
□ In a jitter probe, the remote-ping client sends a series of packets to the remote-ping server at regular intervals (you can set the interval). Once receiving such a packet, the remote-ping server marks it with a timestamp, and then sends it back to the remote-ping client. Upon receiving a packet returned, the remote-ping client computes the delay jitter time. The remote-ping client collects delay jitter statistics on all the packets returned in the test. So, the more packets a jitter probe sends, the more accurate the jitter statistics is, but the longer time the jitter test costs. |
| Interval to send jitter test packets (**jitter-interval**) | Each jitter probe will send multiple UDP test packets at regular intervals (you can set the interval). The smaller the interval is, the faster the test is. But a too small interval may somewhat impact your network. |
| Trap                                                                 | □ A remote-ping test will generate a Trap message no matter whether the test successes or not. You can use the Trap switch to enable or disable the output of trap messages.  
□ You can set the number of consecutive failed remote-ping tests before Trap output. You can also set the number of consecutive failed remote-ping probes before Trap output. |
Remote-ping server configuration tasks

Table 720  Remote-ping server configuration tasks

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Related section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the remote-ping server function</td>
<td>The remote-ping server function is needed only for jitter, TCP, and UDP tests.</td>
<td>“Remote-ping server configuration”</td>
</tr>
<tr>
<td>Configure a listening service on the remote-ping server</td>
<td>You can configure multiple TCP/UDP listening services on one remote-ping server, with each listening service corresponding to a specific destination IP address and port number.</td>
<td>“Remote-ping server configuration”</td>
</tr>
</tbody>
</table>

Remote-ping server configuration

Table 721 describes the configuration on remote-ping server, which is the same for remote-ping test types that need to configure remote-ping server.

Table 721  Remote-ping server configuration

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable the remote-ping server function</td>
<td>remote-ping-server enable</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a UDP listening service</td>
<td>remote-ping-server udpecho ip-address port-num</td>
<td>Required for UDP and jitter tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no UDP listening service is configured.</td>
</tr>
<tr>
<td>Configure a TCP listening service</td>
<td>remote-ping-server tcpconnect ip-address port-num</td>
<td>Required for TCP tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no TCP listening service is configured.</td>
</tr>
</tbody>
</table>

- The remote-ping server function is needed only for jitter, TCP, and UDP tests.
- You can configure multiple TCP/UDP listening services on one remote-ping server, with each listening service corresponding to a specific destination IP address and port number.

Remote-ping Client Configuration

Remote-ping client configuration

After remote-ping client is enabled, you can create multiple test groups for different tests, without the need to enable remote-ping client repeatedly for each test group.

Different types of remote-ping tests are somewhat different in parameters and parameter ranges. The following text describes the configuration on remote-ping client for different test types.

Among the test types supported by remote-ping, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled. With IRF fabric enabled, you are allowed to configure remote-ping tests and use the display commands to check your configurations,
but for non ICMP tests, the remote-ping tests you configured cannot be executed until fabric is disabled.

1 Configuring an ICMP test on remote-ping client

Table 722  Configure ICMP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no test group is configured.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type icmp</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure the destination IP address</td>
<td>destination-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no destination address is configured.</td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td>source-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source IP address is configured.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type icmp</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, each test makes one probe.</td>
</tr>
<tr>
<td>Configure the packet size</td>
<td>datasize size</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the packet size is 56 bytes.</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td>frequency interval</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the type of service (ToS)</td>
<td>tos value</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the service type is zero.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results</td>
<td>Required</td>
</tr>
</tbody>
</table>

2 Configuring a DHCP test on remote-ping client
### Table 723 Configure DHCP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the source interface</td>
<td>source-interface interface-type interface-number</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type dhcp</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results [ admin-name operation-tag ]</td>
<td>Required</td>
</tr>
</tbody>
</table>

Figure 305 Optional

By default, the test type is ICMP.

### Table 724 Configure an FTP test on a remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type ftp</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the destination IP address</td>
<td>destination-ip ip-address</td>
<td>Required</td>
</tr>
</tbody>
</table>
CHAPTER 83: REMOTE-PING CONFIGURATION

4 Configuring an HTTP test on a remote-ping client

Table 724  Configure an FTP test on a remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure the source IP address| source-ip ip-address     | Required
|                                |                          | By default, no source IP address is configured.                             |
| Configure the source port      | source-port port-number  | Optional
|                                |                          | By default, no source port is configured.                                   |
| Configure the number of probes per test | count times | Optional
|                                |                          | By default, each test makes one probe.                                      |
| Configure the maximum number of history records that can be saved | history-records number | Optional
|                                |                          | By default, the maximum number is 50.                                       |
| Configure the automatic test interval | frequency interval | Optional
|                                |                          | By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | timeout time             | Optional
|                                |                          | By default, a probe times out in three seconds.                             |
| Configure the type of service  | tos value                | Optional
|                                |                          | By default, the service type is zero.                                       |
| Configure the type of FTP operation | ftp-operation { get | put } | Optional
|                                |                          | By default, the type of FTP operation is get, that is, the FTP operation will get a file from the FTP server. |
| Configure an FTP login username | username name            | Required
| Configure an FTP login password| password password        | By default, neither username nor password is configured.                    |
| Configure a file name for the FTP operation | filename file-name | Required
|                                |                          | By default, no file name is configured for the FTP operation               |
| Start the test                 | test-enable              | Required
| Display test results           | display remote-ping results [ admin-name operation-tag ] | Required
|                                |                          | You can execute the command in any view.                                   |

Table 725  Configure an HTTP test on a remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 725 Configure an HTTP test on a remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the remote-ping client function</td>
<td><code>remote-ping-agent enable</code></td>
<td>Required. By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td><code>remote-ping administrator-name operation-tag</code></td>
<td>Required. By default, no test group is configured.</td>
</tr>
<tr>
<td>Configure the destination IP address</td>
<td><code>destination-ip ip-address</code></td>
<td>Required. You can configure an IP address or a host name.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td><code>test-type http</code></td>
<td>Required. By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure dns-server</td>
<td><code>dns-server ip-address</code></td>
<td>Required when you use the destination-ip command to configure the destination address as the host name.</td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td><code>source-ip ip-address</code></td>
<td>Optional. By default, no source IP address is configured.</td>
</tr>
<tr>
<td>Configure the source port</td>
<td><code>source-port port-number</code></td>
<td>Optional. By default, no source port is configured.</td>
</tr>
<tr>
<td>Configure the number of probes per test</td>
<td><code>count times</code></td>
<td>Optional. By default, each test makes one probe.</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td><code>history-records number</code></td>
<td>Optional. By default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td><code>frequency interval</code></td>
<td>Optional. By default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td><code>timeout time</code></td>
<td>Optional. By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the type of service</td>
<td><code>tos value</code></td>
<td>Optional. By default, the service type is zero.</td>
</tr>
</tbody>
</table>
CHAPTER 83: REMOTE-PING CONFIGURATION

5 Configuring Jitter Test on Remote-Ping Client

Table 725 Configure an HTTP Test on a Remote-Ping Client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the type of HTTP operation</td>
<td>http-operation { get</td>
<td>post }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the type of HTTP operation is get, that is, the HTTP operation will get data from the HTTP server.</td>
</tr>
<tr>
<td>Configure the HTTP operation string and version in an HTTP test</td>
<td>http-string string version</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, HTTP operation string and version are not configured.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results [ admin-name operation-tag ]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can execute the command in any view.</td>
</tr>
</tbody>
</table>

Table 726 Configure Jitter Test on Remote-Ping Client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no test group is configured.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type jitter</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure the destination IP address</td>
<td>destination-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The destination address must be the IP address of a UDP listening service on the remote-ping server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no destination address is configured.</td>
</tr>
<tr>
<td>Configure the destination port</td>
<td>destination-port</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The destination port must be the port of a UDP listening service on the remote-ping server.</td>
</tr>
<tr>
<td></td>
<td>Port-number</td>
<td></td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td>source-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source IP address is configured.</td>
</tr>
<tr>
<td>Configure the source port</td>
<td>source-port port-number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source port is configured.</td>
</tr>
</tbody>
</table>
Table 726  Configure jitter test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional by default, each test makes one probe.</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Optional by default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the packet size</td>
<td>datasize size</td>
<td>Optional by default, the packet size is 68 bytes.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td>frequency interval</td>
<td>Optional by default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional by default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the type of service</td>
<td>tos value</td>
<td>Optional by default, the service type is zero.</td>
</tr>
<tr>
<td>Configure the number of test packets that will be sent in each jitter probe</td>
<td>jitter-packetnum number</td>
<td>Optional by default, each jitter probe will send 10 packets.</td>
</tr>
<tr>
<td>Configure the interval to send test packets in the jitter test</td>
<td>jitter-interval interval</td>
<td>Optional by default, the interval is 20 milliseconds.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results [ admin-name operation-tag ]</td>
<td>Required by default, you can execute the command in any view.</td>
</tr>
</tbody>
</table>

6 Configuring SNMP test on remote-ping client

Table 727  Configure SNMP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required by default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required by default, no test group is configured.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type snmpquery</td>
<td>Required by default, the test type is ICMP.</td>
</tr>
</tbody>
</table>
CHAPTER 83: REMOTE-PING CONFIGURATION

Configuring TCP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the destination IP</td>
<td>destination-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no destination address is configured.</td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td>source-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source IP address is configured.</td>
</tr>
<tr>
<td>Configure the source port</td>
<td>source-port port-number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source port is configured.</td>
</tr>
<tr>
<td>Configure the number of probes</td>
<td>count times</td>
<td>Optional</td>
</tr>
<tr>
<td>per test</td>
<td></td>
<td>By default, each test makes one probe.</td>
</tr>
<tr>
<td>Configure the maximum number of</td>
<td>history-records number</td>
<td>Figure 311</td>
</tr>
<tr>
<td>history records that can be saved</td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Configure the automatic test</td>
<td>frequency interval</td>
<td>By default, the automatic test interval is zero seconds, indicating no</td>
</tr>
<tr>
<td>interval</td>
<td></td>
<td>automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout</td>
<td>timeout time</td>
<td>Optional</td>
</tr>
<tr>
<td>time</td>
<td></td>
<td>By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the type of service</td>
<td>tos value</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the service type is zero.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results</td>
<td>You can execute the command in any view.</td>
</tr>
<tr>
<td></td>
<td>[admin-name operation-tag]</td>
<td></td>
</tr>
</tbody>
</table>

7 Configuring TCP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter</td>
<td>remote-ping</td>
<td>Required</td>
</tr>
<tr>
<td>its view</td>
<td>administrator-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>operation-tag</td>
<td></td>
</tr>
</tbody>
</table>
Table 728  Configure TCP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the destination address</td>
<td>destination-ip ip-address</td>
<td>Required This IP address and the one configured on the remote-ping server for listening services must be the same. By default, no destination address is configured.</td>
</tr>
<tr>
<td>Configure the destination port</td>
<td>destination-port port-number</td>
<td>Required in a Tcpprivate test A Tcppublic test is a TCP connection test on port 7. Use the remote-ping-server tcpconnect ip-address 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. By default, no destination port number is configured.</td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td>source-ip ip-address</td>
<td>Optional By default, the source IP address is not specified.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type { tcpprivate</td>
<td>tcppublic }</td>
</tr>
<tr>
<td>Configure the source port</td>
<td>source-port port-number</td>
<td>Optional By default, no source port is specified.</td>
</tr>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional By default, one probe is made per time.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td>frequency interval</td>
<td>Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Optional By default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the type of service</td>
<td>tos value</td>
<td>Optional By default, the service type is zero.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
</tbody>
</table>
CHAPTER 83: REMOTE-PING CONFIGURATION

Table 728  Configure TCP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display test results</td>
<td>display remote-ping results</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>[admin-name operation-tag]</td>
<td>The display command can be executed in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any view.</td>
</tr>
</tbody>
</table>

8 Configuring UDP test on remote-ping client

Table 729  Configure UDP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client</td>
<td>remote-ping-agent enable</td>
<td>Required</td>
</tr>
<tr>
<td>function</td>
<td></td>
<td>By default, the remote-ping client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test</td>
<td>remote-ping</td>
<td>Required</td>
</tr>
<tr>
<td>group and enter its view</td>
<td>[administrator-name</td>
<td>By default, no test group is configured.</td>
</tr>
<tr>
<td></td>
<td>operation-tag]</td>
<td></td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type { udpprivate</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>udppublic }</td>
<td>By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure the destination address</td>
<td>destination-ip ip-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This IP address and the one configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on the remote-ping server for listening</td>
</tr>
<tr>
<td></td>
<td></td>
<td>service must be the same.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no destination address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is configured.</td>
</tr>
<tr>
<td>Configure the destination</td>
<td>destination-port</td>
<td>Required</td>
</tr>
<tr>
<td>port</td>
<td>port-number</td>
<td>Required in a Udpprivate test.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A Udppublic test is a UDP connection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test on port 7. Use the remote-ping-server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udppecho ip-address 7 command on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server to configure the listening service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port; otherwise the test will fail. No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port number needs to be configured on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>client; any destination port number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configured on the client will not take</td>
</tr>
<tr>
<td></td>
<td></td>
<td>effect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no destination port number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is configured.</td>
</tr>
<tr>
<td>Configure the source IP</td>
<td>source-ip ip-address</td>
<td>Optional</td>
</tr>
<tr>
<td>address</td>
<td></td>
<td>By default, no source IP address is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configured.</td>
</tr>
<tr>
<td>Configure the source port</td>
<td>source-port port-number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no source port is specified.</td>
</tr>
</tbody>
</table>
Table 729  Configure UDP test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional By default, one probe is made per test.</td>
</tr>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Optional By default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the data packet size</td>
<td>datasync</td>
<td>Optional By default, the data packet size is 100 bytes.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td>frequency interval</td>
<td>Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the service type</td>
<td>tos value</td>
<td>Optional By default, the service type is zero.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results [admin-name operation-tag]</td>
<td>Required The display command can be executed in any view.</td>
</tr>
</tbody>
</table>

Table 730  Configure DNS test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation-tag</td>
<td>Required By default, no test group is configured.</td>
</tr>
<tr>
<td>Configure the source IP address</td>
<td>source-ip ip-address</td>
<td>Optional By default, no source IP address is specified.</td>
</tr>
<tr>
<td>Configure the test type</td>
<td>test-type dns</td>
<td>Required By default, the test type is ICMP.</td>
</tr>
<tr>
<td>Configure the number of probes per test</td>
<td>count times</td>
<td>Optional By default, one probe is made per test.</td>
</tr>
</tbody>
</table>

9 Configuring DNS test on remote-ping client
CHAPTER 83: REMOTE-PING CONFIGURATION

Configuring Remote-ping client to send Trap messages

Traps are generated regardless of whether the remote-ping test succeeds or fails. You can specify whether to output Trap messages by enabling/disabling Trap sending.

Table 730  Configure DNS test on remote-ping client

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the maximum number of history records that can be saved</td>
<td>history-records number</td>
<td>Figure 314  Optional By default, the maximum number is 50.</td>
</tr>
<tr>
<td>Configure the automatic test interval</td>
<td>frequency interval</td>
<td>Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.</td>
</tr>
<tr>
<td>Configure the probe timeout time</td>
<td>timeout time</td>
<td>Optional By default, a probe times out in three seconds.</td>
</tr>
<tr>
<td>Configure the type of service</td>
<td>tos value</td>
<td>Optional By default, the service type is zero.</td>
</tr>
<tr>
<td>Configure the domain name to be resolved</td>
<td>dns resolve-targetdomain name</td>
<td>Required By default, the domain name to be resolved by DNS is not specified.</td>
</tr>
<tr>
<td>Configure the IP address of the DNS server</td>
<td>dns-server ip-address</td>
<td>Required By default, no DNS server address is configured.</td>
</tr>
<tr>
<td>Start the test</td>
<td>test-enable</td>
<td>Required</td>
</tr>
<tr>
<td>Display test results</td>
<td>display remote-ping results [ admin-name operation-tag ]</td>
<td>Required The display command can be executed in any view.</td>
</tr>
</tbody>
</table>

Configure DNS test on remote-ping client

Table 731  Configure the remote-ping client to send Trap messages

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enable the remote-ping client function</td>
<td>remote-ping-agent enable</td>
<td>Required By default, the remote-ping client function is disabled.</td>
</tr>
<tr>
<td>Create a remote-ping test group and enter its view</td>
<td>remote-ping administrator-name operation- tag</td>
<td>Required By default, no test group is configured.</td>
</tr>
<tr>
<td>Enable the remote-ping client to send Trap messages</td>
<td>send-trap { all</td>
<td>{ probefailure</td>
</tr>
<tr>
<td>Configure the number of consecutive unsuccessful remote-ping tests before Trap output</td>
<td>test-failtimes times</td>
<td>Optional By default, Trap messages are sent each time a test fails.</td>
</tr>
</tbody>
</table>
Remote-ping Configuration Example

**ICMP Test**

**Network requirements**
The Switch 5500 serves as the remote-ping client. A remote-ping ICMP test between the switch and another switch uses ICMP to test the round trip time (RTT) for packets generated by the remote-ping client to travel to and back from the destination switch.

**Network diagram**

**Figure 315**  Network diagram for the ICMP test

![Network Diagram]

**Configuration procedure**

- Configure remote-ping Client (Switch A):
  
  ```
  # Enable remote-ping client.
  <5500> system-view
  [5500] remote-ping-agent enable
  
  # Create a remote-ping test group, setting the administrator name to administrator and test tag to ICMP.
  [5500] remote-ping administrator icmp
  
  # Configure the test type as icmp.
  ```

---

**Table 731** Configure the remote-ping client to send Trap messages

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the number of consecutive unsuccessful remote-ping probes before Trap output</td>
<td>probe-failtimes times</td>
<td>Optional By default, Trap messages are sent each time a probe fails.</td>
</tr>
</tbody>
</table>

**Displaying Remote-ping Configuration**

After the above-mentioned configuration, you can use the **display** commands to view the results of the latest test and history information.

**Table 732**  Display remote-ping test results

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display test history</td>
<td>display remote-ping history [ administrator-name operation-tag ]</td>
<td>Available in any view.</td>
</tr>
<tr>
<td>Display the results of the latest test</td>
<td>display remote-ping results [ administrator-name operation-tag ]</td>
<td></td>
</tr>
</tbody>
</table>

---

Remote-ping Configuration Example
[5500-remote-ping-administrator-icmp] test-type icmp

# Configure the destination IP address as 10.2.2.2.
[5500-remote-ping-administrator-icmp] destination-ip 10.2.2.2

# Configure to make 10 probes per test.
[5500-remote-ping-administrator-icmp] count 10

# Set the probe timeout time to 5 seconds.
[5500-remote-ping-administrator-icmp] timeout 5

# Start the test.
[5500-remote-ping-administrator-icmp] test-enable

# Set the maximum number of history records that can be saved to 5.
[5500-remote-ping-administrator-icmp] history-records 5

# Display test results.
[5500-remote-ping-administrator-icmp] display remote-ping results administrator icmp

Remote-ping entry(admin administrator, tag icmp) test result:

  Destination ip address: 10.2.2.2
  Send operation times: 10  Receive response times: 10
  Min/Max/Average Round Trip Time: 3/6/3
  Square-Sum of Round Trip Time: 145
  Last succeeded test time: 2000-04-02 20:55:12.3

  Extend result:
    SD Maximal delay: 0  DS Maximal delay: 0
    Packet lost in test: 0%
    Disconnect operation number: 0  Operation timeout number: 0
    System busy operation number: 0  Connection fail number: 0
    Operation sequence errors: 0  Drop operation number: 0
    Other operation errors: 0

[5500-remote-ping-administrator-icmp] display remote-ping history administrator icmp

Remote-ping entry(admin administrator, tag icmp) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2000-04-02 20:55:12.3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2000-04-02 20:55:12.3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2000-04-02 20:55:12.2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2000-04-02 20:55:12.2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>1</td>
<td>2000-04-02 20:55:12.2</td>
</tr>
</tbody>
</table>

For detailed output description, see the corresponding command manual.

**DHCP Test**

**Network requirements**

Both the remote-ping client and the DHCP server are Switch 5500s. Perform a remote-ping DHCP test between the two switches to test the time required for the remote-ping client to obtain an IP address from the DHCP server.

**Network diagram**

**Figure 316** Network diagram for the DHCP test
Remote-ping Configuration Example

Configuration procedure

- Configure DHCP Server (Switch B):
  Configure DHCP server on Switch B. For specific configuration of DHCP server, refer to “DHCP Server Configuration” on page 601.

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

  <5500> system-view
  [5500] remote-ping-agent enable

  # Create a remote-ping test group, setting the administrator name to administrator and test tag to dhcp.

  [5500] Remote-ping administrator dhcp

  # Configure the test type as dhcp.

  [5500-remote-ping-administrator-dhcp] test-type dhcp

  # Configure the source interface, which must be a VLAN interface. Make sure the DHCP server resides on the network connected to this interface.

  [5500-remote-ping-administrator-dhcp] source-interface Vlan-interface 1

  # Configure to make 10 probes per test.

  [5500-remote-ping-administrator-dhcp] count 10

  # Set the probe timeout time to 5 seconds.

  [5500-remote-ping-administrator-dhcp] timeout 5

  # Start the test.

  [5500-remote-ping-administrator-dhcp] test-enable

  # Display test results

  [5500-remote-ping-administrator-dhcp] display remote-ping results administrator dhcp

  Remote-ping entry (admin administrator, tag dhcp) test result:

  Send operation times: 10 Receive response times: 10
  Min/Max/Average Round Trip Time: 1018/1037/1023
  Square-Sum of Round Trip Time: 10465630
  Last complete test time: 2000-4-3 9:51:30.9

  Extend result:
  SD Maximal delay: 0  DS Maximal delay: 0
  Packet lost in test: 0%
  Disconnect operation number: 0  Operation timeout number: 0
  System busy operation number: 0  Connection fail number: 0
  Operation sequence errors: 0  Drop operation number: 0
  Other operation errors: 0

  [5500-remote-ping-administrator-dhcp] display remote-ping history administrator dhcp

  Remote-ping entry (admin administrator, tag dhcp) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1018</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:51:30.9</td>
</tr>
<tr>
<td>2</td>
<td>1037</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:51:22.9</td>
</tr>
<tr>
<td>3</td>
<td>1024</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:51:18.9</td>
</tr>
<tr>
<td>4</td>
<td>1027</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:51:06.8</td>
</tr>
<tr>
<td>5</td>
<td>1028</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:51:00.8</td>
</tr>
<tr>
<td>6</td>
<td>1020</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:50:52.8</td>
</tr>
<tr>
<td>7</td>
<td>1018</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:50:48.8</td>
</tr>
<tr>
<td>8</td>
<td>1020</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:50:36.8</td>
</tr>
<tr>
<td>9</td>
<td>1020</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:50:30.8</td>
</tr>
<tr>
<td>10</td>
<td>1028</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 09:50:22.8</td>
</tr>
</tbody>
</table>
For detailed output description, see the corresponding command manual.

You can perform a remote-ping DHCP test only when no DHCP client is enabled on any interface. Otherwise, the DHCP Server sends the response to an interface enabled with the DHCP Client rather than to the source interface, thus resulting in remote-ping DHCP test failure.

**FTP Test**

**Network requirements**

Both the remote-ping client and the FTP server are Switch 5500s. Perform a remote-ping FTP test between the two switches to test the connectivity to the specified FTP server and the time required to upload a file to the server after the connection is established. Both the username and password used to log in to the FTP server are **admin**. The file to be uploaded to the server is `cmdtree.txt`.

**Network diagram**

**Figure 317** Network diagram for the FTP test

```
remote-ping Client
    10.1.1.1/8
Switch A

IP network

10.2.2.2/8
Switch B

FTP Server
```

**Configuration procedure**

- Configure FTP Server (Switch B):

  Configure FTP server on Switch B. For specific configuration of FTP server, refer to “FTP and SFTP Configuration” on page 875.

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

  `<5500> system-view
  
  [5500] remote-ping-agent enable

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **FTP**.

  [5500] remote-ping administrator ftp

  # Configure the test type as **ftp**.

  [5500-remote-ping-administrator-ftp] test-type ftp

  # Configure the IP address of the FTP server as 10.2.2.2.

  [5500-remote-ping-administrator-ftp] destination-ip 10.2.2.2

  # Configure the FTP login username.

  [5500-remote-ping-administrator-ftp] username admin

  # Configure the FTP login password.

  [5500-remote-ping-administrator-ftp] password admin

  # Configure the type of FTP operation.

  [5500-remote-ping-administrator-ftp] ftp-operation put

  # Configure a file name for the FTP operation.
```
Remote-ping Configuration Example

[5500-remote-ping-administrator-ftp] filename cmdtree.txt

# Configure to make 10 probes per test.
[5500-remote-ping-administrator-ftp] count 10

# Set the probe timeout time to 30 seconds.
[5500-remote-ping-administrator-ftp] timeout 30

# Configure the source IP address
[5500-remote-ping-administrator-ftp] source-ip 10.1.1.1

# Start the test.
[5500-remote-ping-administrator-ftp] test-enable

# Display test results
[5500-remote-ping-administrator-ftp] display remote-ping results administrator or ftp

Remote-ping entry(administrator, tag ftp) test result:
Destination ip address:10.2.2.2
Send operation times: 10 Receive response times: 10
Min/Max/Average Round Trip Time: 3245/15891/12157
Square-Sum of Round Trip Time: 1644458573
Last complete test time: 2000-4-3 4:0:34.6

Extend result:
SD Maximal delay: 0 DS Maximal delay: 0
Packet lost in test: 0% Disconnect operation number: 0 Operation timeout number: 0
System busy operation number: 0 Connection fail number: 0
Operation sequence errors: 0 Drop operation number: 0
Other operation errors: 0

[5500-remote-ping-administrator-ftp] display remote-ping history administrator or ftp

Remote-ping entry(administrator, tag ftp) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15822</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 04:00:34.6</td>
</tr>
<tr>
<td>2</td>
<td>15772</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 04:00:18.8</td>
</tr>
<tr>
<td>3</td>
<td>9945</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 04:00:02.9</td>
</tr>
<tr>
<td>4</td>
<td>15891</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:59:52.9</td>
</tr>
<tr>
<td>5</td>
<td>15772</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:59:37.0</td>
</tr>
<tr>
<td>6</td>
<td>15653</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:59:21.2</td>
</tr>
<tr>
<td>7</td>
<td>9792</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:59:05.5</td>
</tr>
<tr>
<td>8</td>
<td>9794</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:58:55.6</td>
</tr>
<tr>
<td>9</td>
<td>9891</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:58:45.8</td>
</tr>
<tr>
<td>10</td>
<td>3245</td>
<td>1</td>
<td>0</td>
<td>2000-04-03 03:58:35.9</td>
</tr>
</tbody>
</table>

For detailed output description, see the corresponding command manual.

If you are downloading a file from the server, you do not need to specify an FTP operation type. For details, see “Configuring an FTP test on a remote-ping client”.

**HTTP Test**

**Network requirements**

A 3Com Switch 5500 serves as the Remote-ping client, and a PC serves as the HTTP server. Perform a remote-ping HTTP test between the switch and the HTTP server to test the connectivity and the time required to download a file from the HTTP server after the connection to the server is established.
Network diagram

Figure 318  Network diagram for the HTTP test

Configuration procedure

- Configure the HTTP Server. Use a Windows 2003 Server as the HTTP server and follow the instructions in your Windows 2003 Server documentation.
- Configure remote-ping Client (Switch A):
  # Enable the remote-ping client.
  <5500> system-view
  [5500] remote-ping-agent enable
  # Create a remote-ping test group, setting the administrator name to administrator and test tag to HTTP.
  [5500] Remote-ping administrator http
  # Configure the test type as http.
  [5500-remote-ping-administrator-http] test-type http
  # Configure the IP address of the HTTP server as 10.2.2.2.
  [5500-remote-ping-administrator-http] destination-ip 10.2.2.2
  # Configure to make 10 probes per test.
  [5500-remote-ping-administrator-http] count 10
  # Set the probe timeout time to 30 seconds.
  [5500-remote-ping-administrator-http] timeout 30
  # Start the test.
  [5500-remote-ping-administrator-http] test-enable
  # Display test results
  [5500-remote-ping-administrator-http] display remote-ping results administrator http

Remote-ping entry(admin administrator, tag http) test result:
  Destination ip address: 10.2.2.2
  Send operation times: 10  Receive response times: 10
  Min/Max/Average Round Trip Time: 47/87/74
  Square-Sum of Round Trip Time: 57044
  Last succeeded test time: 2000-4-2 20:41:50.4
Extend result:
  SD Maximal delay: 0  DS Maximal delay: 0
  Packet lost in test: 0%
  Disconnect operation number: 0  Operation timeout number: 0
  System busy operation number: 0  Connection fail number: 0
  Operation sequence errors: 0  Drop operation number: 0
  Other operation errors: 0
Http result:
  DNS Resolve Time: 0  HTTP Operation Time: 675
  DNS Resolve Min Time: 0  HTTP Test Total Time: 748
  DNS Resolve Max Time: 0  HTTP Transmission Successful Times: 10
  DNS Resolve Failed Times: 0  HTTP Transmission Failed Times: 0
  DNS Resolve Timeout Times: 0  HTTP Transmission Timeout Times: 0
Remote-ping Configuration Example

TCP Connect Time: 73  HTTP Operation Min Time: 27
TCP Connect Min Time: 5  HTTP Operation Max Time: 80
TCP Connect Max Time: 20
TCP Connect Timeout Times: 0

[5500-remote-ping-administrator-http] display remote-ping history administrator http
Remote-ping entry(admin administrator, tag http) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.5</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.5</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.5</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.5</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.4</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.4</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.4</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.4</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 15:15:52.4</td>
</tr>
</tbody>
</table>

For detailed output description, see the corresponding command manual.

For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test.

**Jitter Test**

**Network requirements**

Both the remote-ping client and the remote-ping server are Switch 5500s. Perform a remote-ping jitter test between the two switches to test the delay jitter of the UDP packets exchanged between this end (remote-ping client) and the specified destination end (remote-ping server).

**Network diagram**

![Network diagram for the Jitter test](image)

**Figure 319** Network diagram for the Jitter test

**Configuration procedure**

- Configure remote-ping Server (Switch B):
  
  ```
  # Enable the remote-ping server and configure the IP address and port to listen on.
  <5500> system-view
  [5500] remote-ping-server enable
  [5500] remote-ping-server udpecho 10.2.2.2 9000
  ```

- Configure remote-ping Client (Switch A):

  ```
  # Enable the remote-ping client.
  <5500> system-view
  [5500] remote-ping-agent enable
  ```

  ```
  # Create a remote-ping test group, setting the administrator name to administrator and test tag to Jitter.
  [5500] remote-ping administrator Jitter
  ```
CHAPTER 83: REMOTE-PING CONFIGURATION

# Configure the test type as jitter

```
[5500-remote-ping-administrator-Jitter] test-type Jitter
```

# Configure the IP address of the remote-ping server as 10.2.2.2.

```
[5500-remote-ping-administrator-Jitter] destination-ip 10.2.2.2
```

# Configure the destination port on the remote-ping server.

```
[5500-remote-ping-administrator-Jitter] destination-port 9000
```

# Configure to make 10 probes per test.

```
[5500-remote-ping-administrator-http] count 10
```

# Set the probe timeout time to 30 seconds.

```
[5500-remote-ping-administrator-Jitter] timeout 30
```

# Start the test.

```
[5500-remote-ping-administrator-Jitter] test-enable
```

# Display test results

```
[5500-remote-ping-administrator-Jitter] display remote-ping results administrator Jitter
Remote-ping entry(admin administrator, tag Jitter) test result:
Destination ip address: 10.2.2.2
Send operation times: 100 Receive response times: 100
Min/Max/Average Round Trip Time: 9/21/13
Square-Sum of Round Trip Time: 18623
Last complete test time: 2000-4-2 8:14:58.2
Extend result:
SD Maximal delay: 10 DS Maximal delay: 10
Packet lost in test: 0%
Disconnect operation number: 0 Operation timeout number: 0
System busy operation number: 0 Connection fail number: 0
Operation sequence errors: 0 Drop operation number: 0
Other operation errors: 0
Jitter result:
RTT Number: 100
Min Positive SD: 1 Min Positive DS: 1
Max Positive SD: 6 Max Positive DS: 8
Positive SD Number: 38 Positive DS Number: 25
Positive SD Sum: 85 Positive DS Sum: 42
Positive SD average: 2 Positive DS average: 1
Positive SD Square Sum: 267 Positive DS Square Sum: 162
Min Negative SD: 1 Min Negative DS: 1
Max Negative SD: 6 Max Negative DS: 8
Negative SD Number: 30 Negative DS Number: 24
Negative SD Sum: 64 Negative DS Sum: 41
Negative SD average: 2 Negative DS average: 1
Negative SD Square Sum: 200 Negative DS Square Sum: 161
SD lost packets number: 0 DS lost packet number: 0
Unknown result lost packet number: 0
```

```
[5500-remote-ping-administrator-Jitter] display remote-ping history administrator Jitter
Remote-ping entry(admin administrator, tag Jitter) history record:
Index Response Status LastRC Time
1 274 1 0 2000-04-02 08:14:58.2
2 278 1 0 2000-04-02 08:14:57.9
3 280 1 0 2000-04-02 08:14:57.6
4 279 1 0 2000-04-02 08:14:57.3
5 280 1 0 2000-04-02 08:14:57.1
6 270 1 0 2000-04-02 08:14:56.8
7 275 1 0 2000-04-02 08:14:56.5
8 263 1 0 2000-04-02 08:14:56.2
9 270 1 0 2000-04-02 08:14:56.0
10 275 1 0 2000-04-02 08:14:55.7
```
For detailed output description, see the corresponding command manual.

### SNMP Test

#### Network requirements

Both the remote-ping client and the SNMP Agent are Switch 5500s. Perform remote-ping SNMP tests between the two switches to test the time required from Switch A sends an SNMP query message to Switch B (SNMP Agent) to it receives a response from Switch B.

#### Network diagram

**Figure 320** Network diagram for the SNMP test

![Network diagram](remote-ping-client.png)

**Remote-ping Client**

**IP network**

**Switch A**

**Switch B**

**SNMP Agent**

#### Configuration procedure

- **Configure SNMP Agent (Switch B):**
  ```
  # Start SNMP agent and set SNMP version to V2C, read-only community name to public, and read-write community name to private.
  <Sysname> system-view
  [Sysname] snmp-agent
  [Sysname] snmp-agent sys-info version v2c
  [Sysname] snmp-agent community read public
  [Sysname] snmp-agent community write private
  ```

  - The SNMP network management function must be enabled on SNMP agent before it can receive response packets.
  - The SNMPv2c version is used as reference in this example. This configuration may differ if the system uses any other version of SNMP. For details, see SNMP - RMON Operation Manual.

- **Configure remote-ping Client (Switch A):**
  ```
  # Enable the remote-ping client.
  <5500> system-view
  [5500] remote-ping-agent enable
  # Create a remote-ping test group, setting the administrator name to administrator and test tag to snmp.
  [5500] Remote-ping administrator snmp
  # Configure the test type as snmp.
  [5500-remote-ping-administrator-snmp] test-type snmpquery
  # Configure the destination IP address as 10.2.2.2.
  [5500-remote-ping-administrator-snmp] destination-ip 10.2.2.2
  # Configure to make 10 probes per test.
  [5500-remote-ping-administrator-snmp] count 10
  # Set the probe timeout time to 30 seconds.
  ```
TCP Test (Tcpprivate Test) on the Specified Ports

Network requirements
Both the remote-ping client and the remote-ping server are Switch 5500s. Perform a remote-ping Tcpprivate test to test time required to establish a TCP connection between this end (Switch A) and the specified destination end (Switch B), with the port number set to 8000.

Network diagram

![Network diagram for the Tcpprivate test](image)

For detailed output description, see the corresponding command manual.
Remote-ping Configuration Example

Configure remote-ping Client (Switch A):

# Enable the remote-ping client.

<5500> system-view
[5500] remote-ping-agent enable

# Create a remote-ping test group, setting the administrator name to administrator and test tag to tcpprivate.

[5500] Remote-ping administrator tcpprivate

# Configure the test type as tcpprivate.

[5500-remote-ping-administrator-tcpprivate] test-type tcpprivate

# Configure the IP address of the remote-ping server as 10.2.2.2.

[5500-remote-ping-administrator-tcpprivate] destination-ip 10.2.2.2

# Configure the destination port on the remote-ping server.

[5500-remote-ping-administrator-tcpprivate] destination-port 8000

# Configure to make 10 probes per test.

[5500-remote-ping-administrator-tcpprivate] count 10

# Set the probe timeout time to 5 seconds.

[5500-remote-ping-administrator-tcpprivate] timeout 5

# Start the test.

[5500-remote-ping-administrator-tcpprivate] test-enable

# Display test results.

[5500-remote-ping-administrator-tcpprivate] display remote-ping results administrator tcpprivate

Remote-ping entry(administrator, tag tcpprivate) test result:

- Destination ip address: 10.2.2.2
- Send operation times: 10
- Receive response times: 10
- Min/Max/Average Round Trip Time: 4/7/5
- Square-Sum of Round Trip Time: 282
- Last complete test time: 2000-04-02 08:26:02.9

Extend result:

- SD Maximal delay: 0
- DS Maximal delay: 0
- Packet lost in test: 0%
- Disconnect operation number: 0
- Operation sequence errors: 0
- Operation timeout number: 0
- System busy operation number: 0
- Connection fail number: 0
- Other operation errors: 0

[5500-remote-ping-administrator-tcpprivate] display remote-ping history administrator tcpprivate

Remote-ping entry(administrator, tag tcpprivate) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.9</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.8</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.8</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.7</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.7</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.6</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.6</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.5</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.5</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:26:02.4</td>
</tr>
</tbody>
</table>
For detailed output description, see the corresponding command manual.

**Network requirements**
Both the remote-ping client and the remote-ping server are Switch 5500s. Perform a remote-ping Udpprivate test on the specified ports between the two switches to test the RTT of UDP packets between this end (remote-ping client) and the specified destination end (remote-ping server).

**Network diagram**

**Figure 322** Network diagram for the Udpprivate test

---

**UDP Test (Udpprivate Test) on the Specified Ports**

**Configuration procedure**

1. **Configure remote-ping Server (Switch B):**
   
   ```
   <5500> system-view
   [5500] remote-ping-server enable
   [5500] remote-ping-server udpecho 10.2.2.2 8000
   ```

2. **Configure remote-ping Client (Switch A):**
   
   ```
   <5500> system-view
   [5500] remote-ping-agent enable
   # Create a remote-ping test group, setting the administrator name to administrator and test tag to udpprivate.
   [5500] Remote-ping administrator udpprivate
   # Configure the test type as udpprivate.
   [5500-remote-ping-administrator-udpprivate] test-type udpprivate
   # Configure the IP address of the remote-ping server as 10.2.2.2.
   [5500-remote-ping-administrator-udpprivate] destination-ip 10.2.2.2
   # Configure the destination port on the remote-ping server.
   [5500-remote-ping-administrator-udpprivate] destination-port 8000
   # Configure to make 10 probes per test.
   [5500-remote-ping-administrator-udpprivate] count 10
   # Set the probe timeout time to 5 seconds.
   [5500-remote-ping-administrator-udpprivate] timeout 5
   # Start the test.
   [5500-remote-ping-administrator-udpprivate] test-enable
   ```
Remote-ping Configuration Example

Remote-ping Configuration Example

Remote-ping entry(admin administrator, tag udpprivate) test result:
- Destination ip address: 10.2.2.2
- Send operation times: 10 Receive response times: 10
- Min/Max/Average Round Trip Time: 10/12/10
- Square-Sum of Round Trip Time: 1170
- Last complete test time: 2000-4-2 8:29:45.5

Extend result:
- SD Maximal delay: 0
- DS Maximal delay: 0
- Packet lost in test: 0%
- Disconnect operation number: 0 Operation timeout number: 0
- System busy operation number: 0 Connection fail number: 0
- Operation sequence errors: 0 Drop operation number: 0
- Other operation errors: 0

Remote-ping entry(admin administrator, tag udpprivate) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.5</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.4</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.4</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.4</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.4</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.4</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.3</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.3</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.3</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>2000-04-02 08:29:45.3</td>
</tr>
</tbody>
</table>

For detailed output description, see the corresponding command manual.

DNS Test

Network requirements

A Switch 5500 serves as the remote-ping client, and a PC serves as the DNS server. Perform a remote-ping DNS test between the switch and the DNS server to test the time required from the client sends a DNS request to it receives a resolution result from the DNS server.

Network diagram

Figure 323  Network diagram for the DNS test

Configuration procedure

- Use a Windows 2003 Server as the DNS server and follow the instructions in your Windows 2003 Server documentation to configure that server.
- Configure remote-ping Client (Switch A)

  # Enable the remote-ping client.

  <5500> system-view
  [5500] remote-ping-agent enable

  # Create a remote-ping test group, setting the administrator name to administrator and test tag to dns.

  [5500] remote-ping administrator dns
CHAPTER 83: REMOTE-PING CONFIGURATION

# Configure the test type as dns.
[5500-remote-ping-administrator-dns] test-type dns

# Configure the IP address of the DNS server as 10.2.2.2.
[5500-remote-ping-administrator-dns] dns-server 10.2.2.2

# Configure to resolve the domain name www.test.com.

# Configure to make 10 probes per test.
[5500-remote-ping-administrator-dns] count 10

# Set the probe timeout time to 5 seconds.
[5500-remote-ping-administrator-dns] timeout 5

# Start the test.
[5500-remote-ping-administrator-dns] test-enable

# Display test results.
[5500-remote-ping-administrator-dns] display remote-ping results administrator dns

Remote-ping entry(admin administrator, tag dns) test result:
   Destination ip address:10.2.2.2
   Send operation times: 10   Receive response times: 10
   Min/Max/Average Round Trip Time: 6/10/8
   Square-Sum of Round Trip Time: 756
   Last complete test time: 2006-11-28 11:50:40.9

Extend result:
   SD Maximal delay: 0   DS Maximal delay: 0
   Packet lost in test: 0%
   Disconnect operation number: 0   Operation timeout number: 0
   System busy operation number: 0   Connection fail number: 0
   Operation sequence errors: 0   Drop operation number: 0
   Other operation errors: 0

Dns result:
   DNS Resolve Current Time: 10   DNS Resolve Min Time: 6
   DNS Resolve Times: 10   DNS Resolve Max Time: 10
   DNS Resolve Timeout Times: 0   DNS Resolve Failed Times: 0

[5500-remote-ping-administrator-dns] display remote-ping history administrator dns

Remote-ping entry(admin administrator, tag dns) history record:

<table>
<thead>
<tr>
<th>Index</th>
<th>Response</th>
<th>Status</th>
<th>LastRC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
<tr>
<td>10</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>2006-11-28 11:50:40.9</td>
</tr>
</tbody>
</table>

For detailed output description, see the Switch 5500 Family Command Reference Guide.
IPv6 Configuration

- The term router in this document refers to a router in a generic sense or an Ethernet switch running a routing protocol.
- 3Com Switch 5500 Family support IPv6 management features, but do not support IPv6 forwarding and related features.

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.

IPv6 Features

Header format simplification

IPv6 cuts down some IPv4 header fields or moves them to extension headers to reduce the overhead of the basic IPv6 headers. IPv6 uses a fixed-length header, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of the basic IPv6 headers is only twice that of the IPv4 headers (excluding the Options field). For the specific IPv6 header format, see Figure 324.

Figure 324  Comparison between IPv4 header format and IPv6 header format

Adequate address space

The source IPv6 address and the destination IPv6 address are both 128 bits (16 bytes) long. IPv6 can provide $3.4 \times 10^{38}$ addresses to completely 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 source occupied by the IPv6 routing table by means of route aggregation.

Automatic address configuration
To simplify the host configuration, IPv6 supports stateful address configuration and stateless address configuration.

- Stateful address configuration means that a host acquires an IPv6 address and related information from the server (for example, DHCP server).
- Stateless address configuration means that the host automatically configures an IPv6 address and related information based on its own link-layer address and the prefix information issued by the router.

In addition, a host can automatically generate a link-local address based on its own link-layer address and the default prefix (FE80::/64) to communicate with other hosts on the 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 improves the interoperability between different IPv6 applications.

Support for QoS
The Flow Label field in the IPv6 header allows the device to label packets in a flow and provide special handling for these packets.

Enhanced neighbor discovery mechanism
The IPv6 neighbor discovery protocol is implemented by a group of Internet control message protocol version 6 (ICMPv6) messages. The IPv6 neighbor discovery protocol manages message exchange between neighbor nodes (nodes on the same link). The group of ICMPv6 messages takes the place of address resolution protocol (ARP), Internet control message protocol version 4 (ICMPv4), and ICMPv4 redirect messages to provide a series of other functions.

Flexible extension headers
IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the processing efficiency. The Options field in IPv4 packets contains only 40 bytes, while the size of IPv6 extension headers is restricted by that of IPv6 packets.

Introduction to IPv6 Address
IPv6 addresses
An IPv6 address is represented as a series of 16-bit hexadecimals, separated by colons. An IPv6 address is divided into eight groups, 16 bits of each group are represented by four hexadecimal numbers which are separated by colons, 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 shorter format as 2001:0:130F:0:9C0:876A:130B.

If an IPv6 address contains two or more consecutive groups of zeros, they can be replaced by the double-colon :: option. For example, the above-mentioned address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.

**CAUTION:** The double-colon :: can be used only once in an IPv6 address. Otherwise, the device is unable to determine how many zeros the double-colon represents when converting it to zeros to restore the IPv6 address to a 128-bit 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 IPv6-address is an IPv6 address in any of the notations and prefix-length is a decimal number indicating how many bits from the left of an IPv6 address are the address prefix.

**IPv6 address classification**

IPv6 addresses mainly 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 nearest one, according to the routing protocols' measure of distance).

There are no broadcast addresses in IPv6. Their function is superseded by multicast addresses.

The type of an IPv6 address is designated by the format prefix. Table 733 lists the mapping between major address types and format prefixes.

<table>
<thead>
<tr>
<th>Type</th>
<th>Format prefix (binary)</th>
<th>IPv6 prefix ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast address</td>
<td>Unassigned address</td>
<td>::/128</td>
</tr>
<tr>
<td></td>
<td>Loopback address</td>
<td>::/128</td>
</tr>
<tr>
<td></td>
<td>Link-local address</td>
<td>FE80::/10</td>
</tr>
<tr>
<td></td>
<td>Site-local address</td>
<td>FEC0::/10</td>
</tr>
<tr>
<td></td>
<td>Global unicast address</td>
<td>other forms</td>
</tr>
<tr>
<td></td>
<td>Multicast address</td>
<td>FF00::/8</td>
</tr>
</tbody>
</table>
CHAPTER 84: IPV6 CONFIGURATION

Unicast address

There are several forms of unicast address assignment in IPv6, including global unicast address, link-local address, and site-local address.

- The global unicast address, equivalent to an IPv4 public address, is used for aggregatable links and provided for network service providers. This type of address allows efficient routing aggregation to restrict the number of global routing entries.

- The link-local address is used in the neighbor discovery protocol and the stateless auto-configuration. Routers must not forward any packets with link-local source or destination addresses to other links.

- IPv6 unicast site-local addresses are similar to private IPv4 addresses. Routers must not forward any packets with site-local source or destination addresses outside of the site (equivalent to a private network).

- Loopback address: The unicast address 0:0:0:0:0:0:0:1 (represented in shorter 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, but may not use it as a destination IPv6 address.

Multicast address

Multicast addresses listed in Table 734 are reserved for special purpose.

Table 734  Reserved IPv6 multicast addresses

<table>
<thead>
<tr>
<th>Address</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF01::1</td>
<td>Node-local scope all-nodes multicast address</td>
</tr>
<tr>
<td>FF02::1</td>
<td>Link-local scope all-nodes multicast address</td>
</tr>
<tr>
<td>FF01::2</td>
<td>Node-local scope all-routers multicast address</td>
</tr>
<tr>
<td>FF02::2</td>
<td>Link-local scope all-routers multicast address</td>
</tr>
<tr>
<td>FF05::2</td>
<td>Site-local scope all-routers multicast address</td>
</tr>
</tbody>
</table>

Besides, there is another type of multicast address: solicited-node address. The solicited-node multicast address is used to acquire the link-layer addresses of neighbor nodes on the same link and is also used for duplicate address detection. Each IPv6 unicast or anycast address has one corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

FF02:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:1:FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 address.
Interface identifier in IEEE EUI-64 format

Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link and they are required to be unique on that link. Interface identifiers in IPv6 unicast addresses are currently required to be 64 bits long. An interface identifier is derived from the link-layer address of that interface. Interface identifiers in IPv6 addresses are 64 bits long, while MAC addresses are 48 bits long. Therefore, the hexadecimal number FFFE needs to be inserted in the middle of MAC addresses (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 EUI-64 format is obtained.

Figure 325  Convert a MAC address into an EUI-64 address

MAC address: 0012-3400-ABCD

Represented in binary:

```
0000000000010010 0011010000000000 1010101111001101
```

Insert FFFE:

```
0000000000010010 0011010011111111 1111110000000000 1010101111001101
```

Set U/L bit:

```
0000001000010010 0011010011111111 1111110000000000 1010101111001101
```

EUI-64 address: 0212:34FF:FE00:ABCD

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 unreachability detection
- Duplicate address detection
- Router/prefix discovery
- Address autoconfiguration
- Redirection

Table 735 lists the types and functions of ICMPv6 messages used by the NDP.

Table 735  Types and functions of ICMPv6 messages

<table>
<thead>
<tr>
<th>ICMPv6 message</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor solicitation (NS) message</td>
<td>Used to acquire the link-layer address of a neighbor</td>
</tr>
<tr>
<td></td>
<td>Used to verify whether the neighbor is reachable</td>
</tr>
<tr>
<td></td>
<td>Used to perform a duplicate address detection</td>
</tr>
<tr>
<td>Neighbor advertisement (NA) message</td>
<td>Used to respond to a neighbor solicitation message</td>
</tr>
</tbody>
</table>
|                                        | When the link layer address changes, the local node initiates a neighbor advertisement message to notify neighbor nodes of the change.
3Com Switch 5500 Family do not support RS, RA, or Redirect message.

Of the above mentioned IPv6 NDP functions, 3Com Switch 5500 Family support the following three functions: address resolution, neighbor unreachability detection, and duplicate address detection. The subsequent sections present a detailed description of these three functions and relevant configuration.

The NDP mainly provides the following functions:

**Address resolution**

Similar to the ARP function in IPv4, a node acquires the link-layer address of neighbor nodes on the same link through NS and NA messages. Figure 326 shows how node A acquires the link-layer address of node B.

![Figure 326](image)

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 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 the corresponding solicited-node multicast address of its own IPv6 address. If yes, node B learns the link-layer address of node A and returns an NA message containing the link-layer address of node B in the unicast mode.

<table>
<thead>
<tr>
<th>ICMPv6 message</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router solicitation (RS) message</td>
<td>After started, a host sends a router solicitation message to request the router for an address prefix and other configuration information for the purpose of autoconfiguration.</td>
</tr>
<tr>
<td>Router advertisement (RA) message</td>
<td>Used to respond to a router solicitation message. With the RA message suppression disabled, the router regularly sends a router advertisement message containing information such as address prefix and flag bits.</td>
</tr>
<tr>
<td>Redirect message</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 735  Types and functions of ICMPv6 messages

<table>
<thead>
<tr>
<th>ICMP type = 135</th>
<th>Src = A</th>
<th>Dst = solicited-node multicast address of B</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP type = 136</td>
<td>Src = B</td>
<td>Dst = A</td>
</tr>
</tbody>
</table>
3 Node A acquires the link-layer address of node B from the NA message. After that, node A and node B can communicate with each other.

**Neighbor unreachability 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 a node acquires an IPv6 address, it should perform the duplicate address detection to determine whether the address is being used by other nodes (similar to the gratuitous ARP function). The duplication address detection is accomplished through NS and NA messages. Figure 327 shows the duplicate address detection procedure.

![Duplicate address detection](image)

The duplicate address detection procedure is as follows:

1 Node A sends an NS message whose source address is the unassigned address :: and the destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message also 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.

**Introduction to IPv6 DNS**

In the IPv6 network, a Domain Name System (DNS) supporting IPv6 converts domain names into IPv6 addresses. Different from an IPv4 DNS, an IPv6 DNS converts domain names into IPv6 addresses, instead of IPv4 addresses.

However, just like an IPv4 DNS, an IPv6 DNS also covers 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 an IPv4 DNS. For details, refer to “DNS Configuration” on page 1019.
CHAPTER 84: IPV6 CONFIGURATION

Usually, the DNS server connecting IPv4 and IPv6 networks contain not only 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 has the functions of both IPv6 DNS and IPv4 DNS.

Protocols and Standards

Protocol specifications 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 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 3596: DNS Extensions to Support IP Version 6

IPv6 Configuration

Task List

Table 736 Complete these tasks to configure IPv6:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Configuring an IPv6 Unicast Address&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>&quot;Configuring IPv6 NDP&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring a Static IPv6 Route&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring IPv6 TCP Properties&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Configuring IPv6 DNS&quot;</td>
<td>Optional</td>
</tr>
<tr>
<td>&quot;Displaying and Maintaining IPv6&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configuring an IPv6 Unicast Address

An IPv6 address is required for a host to access an IPv6 network. A host can be assigned a global unicast address, a site-local address, or a link-local address.

To enable a host to access a public IPv6 network, you need to assign an IPv6 global unicast address to it.

IPv6 site-local addresses and global unicast addresses can be configured in either of the following ways:

- EUI-64 format: When the EUI-64 format is adopted to form IPv6 addresses, 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.
IPv6 Configuration Task List

- Manual configuration: IPv6 site-local addresses or global unicast addresses are configured manually.

IPv6 link-local addresses can be acquired 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::/64) and the link-layer address of the interface.
- Manual assignment: IPv6 link-local addresses can be assigned manually.

Table 737 Configure an IPv6 unicast address

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td>interface interface-type interface-number</td>
<td>-</td>
</tr>
<tr>
<td>Configure an IPv6 global unicast address</td>
<td>ipv6 address { ipv6-address prefix-length</td>
<td>Use either command By default, no site-local address or global unicast address is configured for an interface. Note that the prefix specified by the prefix-length argument in an EUI-64 address cannot exceed 64 bits in length.</td>
</tr>
<tr>
<td>or site-local address</td>
<td>ipv6-address prefix-length</td>
<td>}</td>
</tr>
<tr>
<td>Adopt the EUI-64 format to form an IPv6 address</td>
<td>ipv6 address ipv6-address prefix-length eui-64</td>
<td>-</td>
</tr>
<tr>
<td>Configure an IPv6 link-local address</td>
<td>ipv6 address auto link-local</td>
<td>Optional By default, after an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be generated automatically.</td>
</tr>
<tr>
<td>Manually assign a link-local address</td>
<td>ipv6 address</td>
<td>-</td>
</tr>
<tr>
<td>Manually assign a link-local address for an interface.</td>
<td>ipv6-address link-local</td>
<td>-</td>
</tr>
</tbody>
</table>

- If an IRF fabric port on a Switch 5500 is enabled with IRF fabric, no IPv6 address can be configured for the switch. To do so, you need to disable the IRF fabric on all IRF fabric ports.

- IPv6 unicast addresses can be configured for only one VLAN interface of Switch 5500. The total number of global unicast addresses and site-local addresses on the VLAN interface can be up to four.

- After an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be 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 link-local address takes effect. If the manually assigned link-local address is deleted, the automatically generated link-local address takes effect.

- The manual assignment takes precedence over the automatic generation. That is, if you first adopt the automatic generation and then the manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt the manual assignment and then the automatic generation, the automatically generated link-local address
CHAPTER 84: IPV6 CONFIGURATION

will not take effect and the link-local address of an interface is still the manually assigned one. If the manually assigned link-local address is deleted, the automatically generated link-local address takes effect.

- You must have carried out the `ipv6 address auto link-local` command before you carry out the `undo ipv6 address auto link-local` command. However, if an IPv6 site-local address or 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 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 statically through manual configuration.

You can configure a static neighbor entry in two ways:

- Mapping a VLAN interface to an IPv6 address and a link-layer address
- Mapping a port in a VLAN to an IPv6 address and a link-layer address

If you configure a static neighbor entry in the second way, make sure the corresponding VLAN interface exists. In this case, the device associates the VLAN interface to the IPv6 address to uniquely identify a static neighbor entry.

Table 738  Configure a static neighbor entry

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure a static neighbor entry</td>
<td>`ipv6 neighbor ipv6-address mac-address (vlan-id port-type port-number</td>
<td>Interface interface-type interface-number)`</td>
</tr>
</tbody>
</table>

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 to the neighbor table. Too large a neighbor table may lead to the forwarding performance degradation of the device. Therefore, 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.

Table 739  Configure the maximum number of neighbors dynamically learned:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum number of neighbors dynamically learned by an interface</td>
<td><code>ipv6 neighbors max-learning-num number</code></td>
<td>Optional</td>
</tr>
</tbody>
</table>

The default value is 2,048.
Configuring the attempts to send an NS message for duplicate address detection

The device sends a neighbor solicitation (NS) message for duplicate address detection. If the device does not receive a response within a specified time (set by the `ipv6 nd ns retrans-timer` command), the device continues to send an NS message. If the device still does not receive a response after the number of attempts to send an NS message reaches the maximum, the device judges the acquired address is available.

### Table 740 Configure the attempts to send an NS message for duplicate address detection

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the attempts to send an NS message for duplicate address detection</td>
<td><code>ipv6 nd dad attempts value</code></td>
<td>Optional 1 by default. When the <code>value</code> argument is set to 0, the duplicate address detection is disabled.</td>
</tr>
</tbody>
</table>

Configuring the NS Interval

After a device sends an NS message, if it does not receive a response within a specific period, the device will send another NS message. You can configure the interval for sending NS messages.

### Table 741 Configure the NS interval

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Specify the NS interval</td>
<td><code>ipv6 nd ns retrans-timer value</code></td>
<td>Optional 1,000 milliseconds by default</td>
</tr>
</tbody>
</table>

Configuring the neighbor reachable timeout time on an interface

After a neighbor passed the reachability detection, the device considers the neighbor to be reachable in a specific period. However, the device will examine whether the neighbor is reachable again when there is a need to send packets to the neighbor after the neighbor reachable timeout time elapsed.

### Table 742 Configure the neighbor reachable timeout time on an interface

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>-</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>-</td>
</tr>
<tr>
<td>Configure the neighbor reachable timeout time</td>
<td><code>ipv6 nd nud reachable-time value</code></td>
<td>Optional 30,000 milliseconds</td>
</tr>
</tbody>
</table>
CHAPTER 84: IPV6 CONFIGURATION

Configuring a Static IPv6 Route
You can configure static IPv6 routes for network interconnection in a small sized IPv6 network.

### Table 743  Configure a static IPv6 route

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure a static IPv6 route</td>
<td>ipv6 route-static ipv6-address prefix-length [ interface-type interface-number] nexthop-address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no static IPv6 route is configured.</td>
</tr>
</tbody>
</table>

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 FIN packets are received, the IPv6 TCP connection status becomes TIME_WAIT. If other packets are received, the finwait timer is reset from the last packet and the connection is terminated after the finwait timer expires.

- **Size of IPv6 TCP receiving/sending buffer**.

### Table 744  Configure IPv6 TCP properties

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set the finwait timer of IPv6 TCP packets</td>
<td>tcp ipv6 timer fin-timeout wait-time</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>675 seconds by default</td>
</tr>
<tr>
<td>Set the synwait timer of IPv6 TCP packets</td>
<td>tcp ipv6 timer syn-timeout wait-time</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>75 seconds by default</td>
</tr>
<tr>
<td>Configure the size of IPv6 TCP receiving/sending buffer</td>
<td>tcp ipv6 window size</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 KB by default</td>
</tr>
</tbody>
</table>

Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time
If too many IPv6 ICMP 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 IPv6 ICMP error packets sent within a specified time. Currently, the token bucket algorithm is adopted.

You can set the capacity of a token bucket, namely, the number of tokens in the bucket. In addition, you can set the update period of the token bucket, namely, the interval for updating the number of tokens in the token bucket to the configured capacity. One token allows one IPv6 ICMP error packet to be sent. Each time an IPv6 ICMP error packet is sent, the number of tokens in a token bucket decreases by 1. If the number of the IPv6 ICMP error packets that are continuously sent out reaches the capacity of the token bucket, the subsequent IPv6 ICMP error packets cannot be sent out until new tokens are put into the token bucket based on the specified update frequency.
Table 745  Configure the maximum number of IPv6 ICMP error packets sent within a specified time

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the maximum number of IPv6 ICMP error packets sent within a specified time</td>
<td>ipv6 icmp-error { bucket bucket-size</td>
<td>ratelimit interval }*</td>
</tr>
</tbody>
</table>

Configuring the hop limit

When sending an IPv6 packet, the device will use this argument to fill in the Hop Limit field in the IPv6 packet header. Upon receipt of the packet, the receiver will also respond a packet carrying with this argument in the Hop Limit field.

Table 746  Configure the hop limit

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure the hop limit</td>
<td>ipv6 nd hop-limit value</td>
<td>Optional 64 by default</td>
</tr>
</tbody>
</table>

Configuring IPv6 DNS

Configuring a static IPv6 DNS entry

You can directly use a host name when applying telnet applications and the system will resolve the host name into an IPv6 address. Each host name can correspond to only one IPv6 addresses. A newly configured IPv6 address will overwrite the previous one.

Table 747  Configure a static host name to IPv6 address mapping

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Configure a static host name to IPv6 address mapping</td>
<td>ipv6 host hostname ipv6-address</td>
<td>Required</td>
</tr>
</tbody>
</table>

Configuring dynamic DNS resolution

If you want to use the dynamic domain name function, you can use the following command to enable the dynamic domain name resolution function. In addition, you should 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 domain name suffix so that you only need to enter some fields of a domain name and the system automatically adds the preset suffix for address resolution. The system can support at most 10 domain name suffixes.

Table 748  Configure dynamic DNS resolution

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>
CHAPTER 84: IPV6 CONFIGURATION

The `dns resolve` and `dns domain` commands are the same as those of IPv4 DNS. For details about the commands, refer to “DNS Configuration” on page 1019.

### Displaying and Maintaining IPv6

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display DNS domain name suffix information</td>
<td><code>display dns domain [ dynamic ]</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display IPv6 dynamic domain name cache information.</td>
<td><code>display dns ipv6 dynamic-host</code></td>
<td></td>
</tr>
<tr>
<td>Display DNS server information</td>
<td><code>display dns server [ dynamic ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the FIB entries</td>
<td><code>display ipv6 fib</code></td>
<td></td>
</tr>
<tr>
<td>Display the mapping between host name and IPv6 address</td>
<td><code>display ipv6 host</code></td>
<td></td>
</tr>
<tr>
<td>Display the brief IPv6 information of an interface</td>
<td>`display ipv6 interface [ interface-type interface-number</td>
<td>brief ]`</td>
</tr>
<tr>
<td>Display neighbor information</td>
<td>`display ipv6 neighbors [ ipv6-address</td>
<td>all</td>
</tr>
<tr>
<td>Display the total number of neighbor entries satisfying the specified conditions</td>
<td>`display ipv6 neighbors [ all</td>
<td>dynamic</td>
</tr>
<tr>
<td>Display information about the routing table</td>
<td><code>display ipv6 route-table [ verbose ]</code></td>
<td></td>
</tr>
<tr>
<td>Display information related to a specified socket</td>
<td><code>display ipv6 socket [ socktype socket-type ] [ task-id socket-id ]</code></td>
<td></td>
</tr>
<tr>
<td>Display the statistics of IPv6 packets and IPv6 ICMP packets</td>
<td><code>display ipv6 statistics</code></td>
<td></td>
</tr>
<tr>
<td>Display the statistics of IPv6 TCP packets</td>
<td><code>display tcp ipv6 statistics</code></td>
<td></td>
</tr>
<tr>
<td>Display the IPv6 TCP connection status</td>
<td><code>display tcp ipv6 status</code></td>
<td></td>
</tr>
<tr>
<td>Display the statistics of IPv6 UDP packets</td>
<td><code>display udp ipv6 statistics</code></td>
<td></td>
</tr>
</tbody>
</table>
The display dns domain and display dns server commands are the same as those of IPv4 DNS. For details about the commands, refer to “DNS Configuration” on page 1019.

**IPv6 Configuration Example**

**IPv6 Unicast Address Configuration**

**Network requirements**

Two switches are directly connected through two Ethernet ports. The Ethernet ports belong to VLAN 2. Different types of IPv6 addresses are configured for the interface VLAN-interface2 on each switch to verify the connectivity between the two switches. The IPv6 prefix in the EUI-64 format is 2001::/64, the global unicast address of Switch A is 3001::1/64, and the global unicast address of Switch B is 3001::2/64.

**Network diagram**

**Figure 328** Network diagram for IPv6 address configuration

![Network diagram](image)

**Configuration procedure**

1. Configure Switch A.

   # Configure an automatically generated link-local address for the interface VLAN-interface2.

   ```
   <SwitchA> system-view
   [SwitchA] interface Vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address auto link-local
   ```

   # Configure an EUI-64 address for the interface VLAN-interface2.

   ```
   [SwitchA-Vlan-interface2] ipv6 address 2001::/64 eui-64
   ```

   # Configure a global unicast address for the interface VLAN-interface2.
2 Configure Switch B.

# Configure an automatically generated link-local address for the interface VLAN-interface2.

<SwitchA> system-view
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address auto link-local

# Configure an EUI-64 address for the interface VLAN-interface2.

[SwitchB-Vlan-interface2] ipv6 address 2001::/64 eui-64

# Configure a global unicast address for the interface VLAN-interface2.

[SwitchB-Vlan-interface2] ipv6 address 3001::2/64

Verification

# Display the brief IPv6 information of an interface on Switch A.

[SwitchA-Vlan-interface2] display ipv6 interface vlan-interface 2
Vlan-interface2 current state : UP
Line protocol current state : UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE49:8048
    Global unicast address(es):
          2001::20F:E2FF:FE49:8048, subnet is 2001::/64
          3001::1, subnet is 3001::/64
    Joined group address(es):
          FF02::1:FF00:1
          FF02::1:FF49:8048
          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

# Display the brief IPv6 information of the interface on Switch B.

[SwitchB-Vlan-interface2] display ipv6 interface Vlan-interface 2
Vlan-interface2 current state : UP
Line protocol current state : UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1
    Global unicast address(es):
          2001::20F:E2FF:FE00:1, subnet is 2001::/64
          3001::2, subnet is 3001::/64
    Joined group address(es):
          FF02::1:FF00:2
          FF02::1:FF00:1
          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
# On Switch A, ping the link-local address, EUI-64 address, and global unicast address of Switch B. If the configurations are correct, the above three types of IPv6 addresses can be pinged.

**CAUTION:** When you use the `ping ipv6` command to verify the reachability of the destination, you must specify the `-i` keyword if the destination address is a link-local address. For the operation of IPv6 ping, refer to “IPv6 Ping” on page 1013.

```
[SwitchA-Vlan-interface2] ping ipv6 FE80::20F:E2FF:FE00:1 -i Vlan-interface 2
PING FE80::20F:E2FF:FE00:1 : 56 data bytes, press ESCAPE KEY to break
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=1 hop limit=255 time = 80 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=2 hop limit=255 time = 60 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=4 hop limit=255 time = 70 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=5 hop limit=255 time = 60 ms
--- FE80::20F:E2FF:FE00:1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 60/66/80 ms
```

```
[SwitchA-Vlan-interface2] ping ipv6 2001::20F:E2FF:FE00:1
PING 2001::20F:E2FF:FE00:1 : 56 data bytes, press ESCAPE KEY to break
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=1 hop limit=255 time = 40 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=2 hop limit=255 time = 70 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=4 hop limit=255 time = 60 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=5 hop limit=255 time = 60 ms
--- 2001::20F:E2FF:FE00:1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 40/58/70 ms
```

```
[SwitchA-Vlan-interface2] ping ipv6 3001::2
PING 3001::2 : 56 data bytes, press ESCAPE KEY to break
Reply from 3001::2
bytes=56 Sequence=1 hop limit=255 time = 50 ms
Reply from 3001::2
bytes=56 Sequence=2 hop limit=255 time = 60 ms
Reply from 3001::2
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from 3001::2
```

bytes=56 Sequence=4 hop limit=255 time = 70 ms
Reply from 3001::2
bytes=56 Sequence=5 hop limit=255 time = 60 ms

--- 3001::2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 50/60/70 ms
IPv6 APPLICATION CONFIGURATION

Introduction to IPv6 Application
IPv6 are supporting more and more applications. Most of IPv6 applications are the same as those of IPv4. The applications supported on 3Com Switch 5500 Family are:
- Ping
- Traceroute
- TFTP
- Telnet

Configuring IPv6 Application

IPv6 Ping
The ping ipv6 command is commonly used for testing the reachability of a host. This command sends an ICMPv6 message to the destination host and records the time for the response message to be received. For details about the ping command, refer to “Basic System Configuration and Debugging” on page 929.

Table 750 Ping IPv6

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>

⚠️ CAUTION: When you use the ping ipv6 command to verify the reachability of the destination, you must specify the -i keyword if the destination address is a link-local address.

IPv6 Traceroute
The traceroute ipv6 command is used to record the route of IPv6 packets from source to destination, so as to check whether the link is available and determine the point of failure.
As Figure 329 shows, the traceroute process is as follows:

- The source sends an IP datagram with the Hop Limit of 1.
- If the first hop device receiving the datagram reads the Hop Limit of 1, it will discard the packet and return an ICMP timeout error message. Thus, the source can get the first device’s address in the route.
- The source sends a datagram with the Hop Limit of 2 and the second hop device returns an ICMP timeout error message. The source gets the second device’s address in the route.
- This process continues until the datagram reaches the destination host. As there is no application using the UDP port, the destination returns a port unreachable ICMP error message.
- The source receives the port unreachable ICMP error message and understands that the packet has reached the destination, and thus determines the route of the packet from source to destination.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceroute IPv6</td>
<td>tracert ipv6</td>
<td>-f first-ttl</td>
</tr>
</tbody>
</table>
CAUTION: When you use the tftp ipv6 command to connect to the TFTP server, you must specify the -i keyword if the destination address is a link-local address.

IPv6 Telnet

Telnet protocol belongs to application layer protocols of the TCP/IP protocol suite, and is used to provide remote login and virtual terminals. The device can be used either as a Telnet client or a Telnet server.

As the following figure shows, the Host is running Telnet client application of IPv6 to set up an IPv6 Telnet connection with Device A, which serves as the Telnet server. If Device A again connects to Device B through Telnet, the Device A is the Telnet client and Device B is the Telnet server.

Figure 330  Provide Telnet services

Configuration prerequisites

Enable Telnet on the Telnet server and configure the authentication method. For details, refer to "Logging into an Ethernet Switch" on page 31.

Table 753  Set up IPv6 Telnet connections

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform the telnet command on the Telnet client to log in to other devices</td>
<td>telnet ipv6 remote-system [-i interface-type interface-number] [-p port-number]</td>
<td>Required Available in user view</td>
</tr>
</tbody>
</table>

CAUTION: When you use the telnet ipv6 command to connect to the Telnet server, you must specify the -i keyword if the destination address is a link-local address.

Displaying and maintaining IPv6 Telnet

Table 754  Display and maintain IPv6 Telnet

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the use information of the users who have logged in</td>
<td>display users [ all ]</td>
<td>Available in any view</td>
</tr>
</tbody>
</table>
IPv6 Application Configuration Example

IPv6 Applications

Network requirements

In Figure 331, SWA, SWB, and SWC are three switches, among which SWA is a Switch 5500, SWB and SWC are two switches supporting IPv6 forwarding. In a LAN, there is a Telnet server and a TFTP server for providing Telnet service and TFTP service to the switch respectively. It is required that you telnet to the telnet server from SWA and download files from the TFTP server.

Network diagram

Figure 331  Network diagram for IPv6 applications

Configuration procedure

You need configure IPv6 address at the switch’s and server’s interfaces and ensure that the route between the switch and the server is accessible before the following configuration.

# Ping SWB’s IPv6 address from SWA.

SWA> ping ipv6 3003::1
PING 3003::1 : 64 data bytes, press CTRL_C to break
Reply from 3003::1 bytes=56 Sequence=1 hop limit=64 time = 110 ms
Reply from 3003::1 bytes=56 Sequence=2 hop limit=64 time = 31 ms
Reply from 3003::1 bytes=56 Sequence=3 hop limit=64 time = 31 ms
Reply from 3003::1 bytes=56 Sequence=4 hop limit=64 time = 31 ms
Reply from 3003::1 bytes=56 Sequence=5 hop limit=64 time = 31 ms
--- 3003::1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/46/110 ms

# On SWA, configure static routes to SWC, the Telnet Server, and the TFTP Server.

<SWA> system-view
[SWA] ipv6 route-static 3002:: 64 3003::1
[SWA] ipv6 route-static 3001:: 64 3003::1
[SWA] quit

# Trace the IPv6 route from SWA to SWC.

<SWA> tracert ipv6 3002::1
traceroute to 3002::1 30 hops max, 60 bytes packet
1 3003::1 30 ms 0 ms 0 ms
2 3002::1 10 ms 10 ms 0 ms

# SWA downloads a file from TFTP server 3001::3.

<SWA> tftp ipv6 3001::3 get filetoget flash:/filegothere
.  
File will be transferred in binary mode
Downloading file from remote tftp server, please wait....
TFTP: 13 bytes received in 1.243 second(s)
File downloaded successfully.

# SWA Connect to Telnet server 3001::2.

<SWA> telnet ipv6 3001::2
Trying 3001::2...
Press CTRL+K to abort
Connected to 3001::2...
Telnet Server>

# Set up a Telnet connection from SWA to SWC.

<SWA> telnet ipv6 3002::1
Trying 3002::1...
Press CTRL+K to abort
Connected to 3002::1...

Troubleshooting IPv6 Application

Unable to Ping a Remote Destination

Symptom
Unable to ping a remote destination and return an error message.
**Solution**
- Check that the IPv6 addresses are configured correctly.
- Use the `display ipv6 interface` command to determine the interfaces of the source and the destination and the link-layer protocol between them are up.
- Use the `display ipv6 route-table` command to verify that the destination is reachable.
- Use the `ping ipv6 -t timeout { destination-ipv6-address | hostname } [ -i interface-type interface-number ]` command to increase the timeout time limit, so as to determine whether it is due to the timeout limit is too small.

**Unable to Run Traceroute**

**Symptom**
Unable to trace the route by performing traceroute operations.

**Solution**
- Check that the destination host can be pinged.
- If the host can be pinged through, check whether the UDP port that was included in the `tracert ipv6` command is used by an application on the host. If yes, you need to use the `tracert ipv6` command with an unreachable UDP port.

**Unable to Run TFTP**

**Symptom**
Unable to download and upload files by performing TFTP operations.

**Solution**
- Check that the route between the device and the TFTP server is up.
- Check that the file system of the device is usable. You can check it by running the `dir` command in user view.
- Check that the ACL configured for the TFTP server does not block the connection to the TFTP server.

**Unable to Run Telnet**

**Symptom**
Unable to login to Telnet server by performing Telnet operations.

**Solution**
- Check that the Telnet server application is running on the server. Check the configuration allows the server reachable.
- Check that the route between the device and the TFTP server is up.
This chapter covers only IPv4 DNS configuration. For details on IPv6 DNS, refer to “IPv6 Configuration” on page 995.

DNS Overview

Domain Name System (DNS) is a mechanism used for TCP/IP applications to provide domain name-to-IP address translation. With DNS, you can use memorizable and meaningful domain names in some applications and let the DNS server resolve it into correct IP addresses.

There are two types of DNS services, static and dynamic. Each time the DNS server receives a name query, it checks its static DNS database before looking up the dynamic DNS database. Reduction of the searching time in the dynamic DNS database would increase efficiency. Some frequently used addresses can be put in the static DNS database.

Currently, the Switch 5500 supports both static and dynamic DNS clients.

Static Domain Name Resolution

The static domain name resolution means manually setting up mappings between domain names and IP addresses. IP addresses of the corresponding domain names can be found in the static domain name resolution table for applications, such as Telnet.

Dynamic Domain Name Resolution

Resolution 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 in 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 the query to the DNS server.
3. The DNS server looks up its DNS database for a match. If no match is found, it sends a query to a higher-level DNS server. This process continues until a result, success or failure, is returned.
4. The DNS client performs the next operation according to the result.
Figure 332 Dynamic domain name resolution

Figure 332 shows the relationship between user program, DNS client, and DNS server.

The resolver and cache comprise the DNS client. The user program and DNS client run on the same device, 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 name and IP address in the dynamic domain name cache of the DNS client. There is no need to send a request to the DNS server for a repeated query request 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 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 not complete. The resolver can supply the missing part (automatic domain name addition). 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, such as aabbcc, the resolver will consider this as a host name and add a DNS suffix before processing. The original name such as aabbcc is used if all DNS lookups fail.
- If there is a period in the domain name, such as www.aabbcc or aabbcc., it indicates that no DNS suffix needs to be added and the resolver uses this domain name to perform the first DNS lookup. If the lookup fails, the resolver adds a DNS suffix for another lookup.
## Configuring Domain Name Resolution

### Configuring Static Domain Name Resolution

**Table 755**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Configure a mapping</td>
<td><strong>ip host hostname ip-address</strong></td>
<td>Required</td>
</tr>
<tr>
<td>between a host name and an IP address</td>
<td></td>
<td>No IP address is assigned to a host name by default.</td>
</tr>
</tbody>
</table>

The IP address you assign to a host name last time 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

**Table 756**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the system view</td>
<td><strong>system-view</strong></td>
<td>-</td>
</tr>
<tr>
<td>Enable dynamic domain name resolution</td>
<td><strong>dns resolve</strong></td>
<td>Required</td>
</tr>
<tr>
<td>Configure an IP address for the DNS server</td>
<td><strong>dns server ip-address</strong></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No IP address is configured for the DNS server by default.</td>
</tr>
<tr>
<td>Configure DNS suffixes</td>
<td><strong>dns domain domain-name</strong></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No DNS suffix is configured by default</td>
</tr>
</tbody>
</table>

You may configure up to six DNS servers and ten DNS suffixes.

### Displaying and Maintaining DNS

After completing the above configuration, you can execute the **display** command and the **nslookup type** command in any view to display the DNS configuration information and the DNS resolution result to verify the configuration effect. You can execute the **reset** command in user view to clear the information stored in the dynamic domain name resolution cache.
### Table 757  Display and maintain DNS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display static DNS database</td>
<td>display ip host</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the DNS server information</td>
<td>display dns server [ dynamic ]</td>
<td></td>
</tr>
<tr>
<td>Display the DNS suffixes</td>
<td>display dns domain [ dynamic ]</td>
<td></td>
</tr>
<tr>
<td>Display the information in the dynamic domain name cache</td>
<td>display dns dynamic-host</td>
<td></td>
</tr>
<tr>
<td>Display the DNS resolution result</td>
<td>nslookup type { ptr ip-address</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Clear the information in the dynamic domain name cache</td>
<td>a domain-name }</td>
<td></td>
</tr>
</tbody>
</table>

### DNS Configuration Examples

#### Static Domain Name Resolution Configuration Example

**Network requirements**
The switch uses static domain name resolution to access host 10.1.1.2 through domain name host.com.

**Network diagram**

![Network diagram for static DNS configuration](image)

**Configuration procedure**

# Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<5500> system-view
[5500] ip host host.com 10.1.1.2
```

# Execute the **ping host.com** command to verify that the device can use static domain name resolution to get the IP address 10.1.1.2 corresponding to host.com.

```
[5500] 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=127 time=3 ms
  Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=127 time=3 ms
  Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=127 time=2 ms
  Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=127 time=5 ms
  Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=127 time=3 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
```
Dynamic Domain Name Resolution Configuration Example

Network requirements
As shown in Figure 334, the switch serving as a DNS client uses dynamic domain name resolution to access the host at 3.1.1.1/16 through its domain name `host`. The DNS server has the IP address 2.1.1.2/16. The DNS suffix is `com`.

Network diagram

Figure 334  Network diagram for dynamic DNS configuration

Configuration procedure

Before doing the following configuration, make sure that:

- The routes between the DNS server, Switch, and Host are reachable.
- Necessary configurations are done on the devices. For the IP addresses of the interfaces, see the figure above.
- There is a mapping between domain name `host` and IP address 3.1.1.1/16 on the DNS server.
- The DNS server works normally.

# Enable dynamic domain name resolution.

```
<5500> system-view
[5500] dns resolve
```

# Configure the IP address 2.1.1.2 for the DNS server.

```
[5500] dns server 2.1.1.2
```

# Configure com as the DNS suffix

```
[5500] dns domain com
```

Execute the `ping host` command on Switch to verify that the communication between Switch and Host is normal and that the corresponding IP address is 3.1.1.1.

```
[5500] ping host
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=125 time=4 ms
```
Troubleshooting DNS

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 check that the specified domain name is in the cache.
- If there is no defined domain name, check that dynamic domain name resolution is enabled and the DNS client can communicate with the DNS server.
- If the specified domain name exists in the cache but the IP address is incorrect, check that the DNS client has the correct IP address of the DNS server.
- Check that the mapping between the domain name and IP address is correct on the DNS server.
Smart Link Overview

As shown in Figure 335, dual-uplink networking is widely applied currently. Usually, Spanning Tree Protocol (STP) is used to implement link redundancy backup in the network. However, STP is not suitable for users with a high demand for convergence time. Smart Link can achieve active/standby link redundancy backup and fast convergence to meet the user demand.

Smart Link has the following features:

- Active/standby backup for dual-uplink networking
- Simple configuration and operation

Basic Concepts in Smart Link

Smart Link group

A Smart Link group consists of two member ports, one master port and one slave port. Normally, only one port (master or slave) is active, and the other port is blocked, that is, in the standby state. When link failure occurs on the port in active state, the Smart Link group will block the port automatically and turn standby state to active state on the blocked port.

Figure 335  Network diagram of Smart Link

In Figure 335, Ethernet 1/0/1 and Ethernet 1/0/2 on Switch A are two member ports of a Smart Link group.

Master port

The master port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet 1/0/1 of switch A in Figure 335 as the master port through the command line.
Slave port
The slave port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet 1/0/2 of switch A in Figure 335 as the slave port through the command line.

Flush message
When a forwarding link fails, the device will switch the traffic to the blocked standby link. The former forwarding entries of each device in the network are no longer suitable for the new topology, so MAC address forwarding entries and ARP entries must be updated throughout the network. In this case, the Smart Link group sends flush messages to notify other devices to refresh MAC address forwarding entries and ARP entries.

Control VLAN for sending flush messages
This control VLAN sends flush messages. When link switching occurs, the device (Switch A in Figure 335) broadcasts flush messages in this control VLAN.

Control VLAN for receiving flush messages
This control VLAN is used for receiving and processing flush messages. When link switching occurs, the devices (Switch B and Switch C in Figure 335) receive and process flush messages of this control VLAN, and then refresh MAC forwarding table entries and ARP entries.

- Currently, the member ports of a Smart Link group cannot be dynamic link aggregation groups.
- If the master port or slave port of a Smart Link group is a link aggregation group, you cannot remove this link aggregation group directly or change the aggregation group into a dynamic aggregation group. Before removing this aggregation group, you must unbind the link aggregation group from the Smart Link.

Operating Mechanism of Smart Link

Figure 336  Network diagram of Smart Link operating mechanism
As shown in Figure 336, Ethernet 1/0/1 on Switch A is active and Ethernet 1/0/2 on Switch A is blocked. When the link connected to Ethernet 1/0/1 fails, Ethernet 1/0/1 is blocked automatically, and the state of Ethernet 1/0/2 turns to active state.

- When link switching occurs in the Smart Link group, MAC forwarding entries and ARP entries of each device in the network may be out of date. In order to guarantee correct packet transmission, you must enable the Smart Link device to send flush messages to notify the other devices in the network to refresh their own MAC forwarding entries and ARP entries. In this case, all the uplink devices must be capable of identifying flush messages from the Smart Link group and refreshing MAC forwarding entries and ARP entries.

- On a Smart Link-enabled device, if a port is blocked due to link failure, the port remains blocked after the link recovers from the failure, and does not preempt the traffic resource. Therefore, the traffic stays stable. The port does not come into the forwarding state until the next link switching.

### Configuring Smart Link

**Before configuring a member port of a Smart Link group, you must:**

- Disable the port to avoid loops, thus preventing broadcast storm.
- Disable STP on the port and its peer port.

After completing the configuration, you need to enable the Ethernet ports disabled before configuring the Smart Link group.

### Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Configuring a Smart Link Device”</td>
<td>Required</td>
</tr>
<tr>
<td>Create a Smart Link group</td>
<td></td>
</tr>
<tr>
<td>Add member ports to the Smart Link group</td>
<td></td>
</tr>
<tr>
<td>Enable the function of sending flush messages in the specified control VLAN</td>
<td></td>
</tr>
<tr>
<td>“Configuring Associated Devices”</td>
<td>Required</td>
</tr>
<tr>
<td>Enable the function of processing flush messages received from the specified control VLAN</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Smart Link Device

A Smart Link device refers to a device on which Smart Link is enabled and a Smart Link group is configured, and that sends flush messages from the specified control VLAN. A member port of a Smart Link group can be either an Ethernet port or a manually-configured or static LACP aggregation group. You can configure a port or a link aggregation group as a member of a Smart Link group.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a Smart Link group and enter Smart Link group view</td>
<td>smart-link group group-id</td>
<td>Required</td>
</tr>
</tbody>
</table>
CHAPTER 87: SMART LINK CONFIGURATION

Configuring Associated Devices

An associated device mentioned in this document refers to a device that supports Smart Link and locally configured to process flush messages received from the specified control VLAN so as to work with the corresponding Smart Link device. As shown in Figure 336, all the devices including Switch C, Switch D, and Switch E on the active and backup links connecting the Smart Link device (Switch A) and the target uplink device (Switch E) are all associated devices.

However, you do not have to enable all the ports of an associated device to process flush messages received from the specified control VLAN. You need to enable this function only on the ports that are on the active and backup links connecting the Smart Link device and the target device. As shown in Figure 336, you need to enable this function on Ethernet 1/0/1 and Ethernet 1/0/2 of Switch C, Ethernet 1/0/1 and Ethernet 1/0/2 of Switch D, and Ethernet 11/0/1 and Ethernet 1/0/12 of Switch E.

Table 760 Configure Smart Link (with link aggregation groups are the members of the Smart Link group)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a Smart Link group and enter Smart Link group view</td>
<td>smart-link group group-id</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a link aggregation group as a member of the Smart Link group</td>
<td>link-aggregation group group-id { master</td>
<td>slave }</td>
</tr>
<tr>
<td>Enable the function of sending flush messages in the specified control VLAN</td>
<td>flush enable control-vlan vlan-id</td>
<td>Optional</td>
</tr>
</tbody>
</table>

By default, no control VLAN for sending flush messages is specified.

Table 761 Enable the specified port to process flush messages received from the specified control VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
</tbody>
</table>

By default, no control VLAN for sending flush messages is specified.
Table 761 Enable the specified port to process flush messages received from the specified control VLAN

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>System view</td>
<td><code>smart-link flush enable control-vlan vlan-id port interface-type interface-number [ to interface-type interface-number ]</code></td>
<td>Required, use either approach. By default, no control VLAN for receiving flush messages is specified.</td>
</tr>
<tr>
<td>Ethernet port view</td>
<td><code>interface interface-type interface-number smart-link flush enable control-vlan vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>
process flush messages. The function of processing flush messages must be manually configured for each port in the aggregation group.

- The VLAN configured as a control VLAN to send and receive flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as the control VLAN for the Smart Link group, this VLAN will become a static VLAN, and the prompt information is displayed.

### Displaying and Maintaining Smart Link

After the above-mentioned configuration, you can use the following `display` commands in any view to view the Smart Link group information and the statistics information of flush messages received and processed by current device, so as to verify the configuration.

Use the `reset` command in user view to clear flush message statistics.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information of a Smart Link group</td>
<td>`display smart-link group { group-id</td>
<td>all }`</td>
</tr>
<tr>
<td>Display the statistics information of flush messages received and processed by the current device</td>
<td><code>display smart-link flush</code></td>
<td></td>
</tr>
<tr>
<td>Clear flush message statistics</td>
<td><code>reset smart-link packets counter</code></td>
<td>You can execute the <code>reset</code> command in user view.</td>
</tr>
</tbody>
</table>

### Smart Link Configuration Example

**Implementing Link Redundancy Backup**

**Network requirements**

As shown in Figure 337, Switch A is a 3Com Switch 5500. Switch C, Switch D and Switch E support Smart Link. Configure Smart Link feature to provide remote PCs with reliable access to the server.
Network diagram

Figure 337  Network diagram for Smart Link configuration

Configuration procedure

1  Configure a Smart Link group on Switch A and configure member ports for it. Enable the function of sending flush messages in Control VLAN 1.

   # Enter system view.
   <switchA> system-view
   # Enter Ethernet port view. Disable STP on Ethernet 1/0/1 and Ethernet 1/0/2.
   [SwitchA] interface Ethernet 1/0/1
   [SwitchA-Ethernet1/0/1] stp disable
   [SwitchA-Ethernet1/0/1] quit
   [SwitchA] interface Ethernet 1/0/2
   [SwitchA-Ethernet1/0/2] stp disable
   [SwitchA-Ethernet1/0/2] quit
   # Return to system view.
   [SwitchA-Ethernet1/0/2]quit
   # Create Smart Link group 1 and enter the corresponding Smart Link group view.
   [SwitchA] smart-link group 1
   # Configure Ethernet1/0/1 as the master port and Ethernet 1/0/2 as the slave port for Smart Link group 1.
   [SwitchA-smlk-group1] port Ethernet 1/0/1 master
   [SwitchA-smlk-group1] port Ethernet 1/0/2 slave
   # Configure to send flush messages within VLAN 1.
   [SwitchA-smlk-group1] flush enable control-vlan 1

2  Enable the function of processing flush messages received from VLAN 1 on Switch C.

   # Enter system view.
<SwitchC> system-view
# Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2.
<SwitchC> smart-link flush enable control-vlan 1 port Ethernet 1/0/1 to Ethernet 1/0/2

3 Enable the function of processing flush messages received from VLAN 1 on Switch D.

# Enter system view.
<SwitchD> system-view
# Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2.
[SwitchD] smart-link flush enable control-vlan 1 port Ethernet 1/0/1 to Ethernet 1/0/2

4 Enable the function of processing flush messages received from VLAN 1 on Switch E.

# Enter system view.
<SwitchE> system-view
# Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2 and Ethernet 1/0/3.
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 1/0/2 to Ethernet 1/0/3
**Introduction to Monitor Link**

Monitor Link is a collaboration scheme introduced to complement for Smart Link. It is used to monitor uplink and to perfect the backup function of Smart Link.

A monitor Link consists of an uplink port and one or multiple downlink ports. When the link for the uplink port of a Monitor Link group fails, all the downlink ports in the Monitor Link group are forced down. When the link for the uplink port recovers, all the downlink ports in the group are re-enabled.

Figure 338  Network diagram for a Monitor Link group implementation

As shown in Figure 338, the Monitor Link group configured on the device Switch A consists of an uplink port (Ethernet 1/0/1) and two downlink ports (Ethernet 1/0/2 and Ethernet 1/0/3). A member port can be an Ethernet port, static LACP aggregation group, manual link aggregation group, or Smart Link group. A Smart Link group can serve as the uplink port only.
How Monitor Link Works

As shown in Figure 339, the devices Switch C and Switch D are connected to the uplink device Switch E. Switch C is configured with a Monitor Link group, where Ethernet 1/0/1 is the uplink port, while Ethernet 1/0/2 and Ethernet 1/0/3 are the downlink ports. Switch A is configured with a Smart Link group, where Ethernet 1/0/1 is the master port and Ethernet 1/0/2 is the slave port.

- If Switch C is not configured with Monitor Link group, when the link for the uplink port Ethernet 1/0/1 on Switch C fails, the links in the Smart Link group are not switched because the link for the master port Ethernet 1/0/1 of Switch A configured with Smart Link group operates normally. Actually, however, the traffic on Switch A cannot be up-linked to Switch E through the link of Ethernet 1/0/1.

- If Switch C is configured with Monitor Link group and Monitor Link group detects that the link for the uplink port Ethernet 1/0/1 fails, all the downlink ports in the group are shut down; therefore, Ethernet 1/0/3 on Switch C is blocked. Now, Smart Link group configured on Switch A detects that a link fault occurs on the master port Ethernet 1/0/1. Then, Smart Link immediately activates the slave port Ethernet 1/0/2 so that traffic is switched to the backup link.

- Currently, member ports of a Monitor Link group cannot be dynamic link aggregation groups.

- If the uplink or downlink port in the Monitor Link group is a link aggregation group, you cannot directly delete this aggregation group or change this aggregation group into a dynamic aggregation group. To delete this aggregation group, you must first unbind this aggregation group from the Monitor Link.

Configuring Monitor Link

Before configuring a Monitor Link group, you must create a Monitor Link group and configure member ports for it. A Monitor Link group consists of an uplink port...
and one or multiple downlink ports. The uplink port can be a manually-configured or static LACP link aggregation group, an Ethernet port, or a Smart Link group. The downlink ports can be manually-configured link aggregation groups or static LACP link aggregation groups, or Ethernet ports.

### Configuration Tasks

**Table 763** Monitor Link configuration tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Creating a Monitor Link Group”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring the Uplink Port”</td>
<td>Required</td>
</tr>
<tr>
<td>“Configuring a Downlink Port”</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Creating a Monitor Link Group**

**Table 764** Create a Monitor Link group

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Create a Monitor Link group</td>
<td>monitor-link group group-id</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring the Uplink Port**

**Table 765** Configure the uplink port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter the specified Monitor Link group view</td>
<td>monitor-link group group-id</td>
<td>-</td>
</tr>
<tr>
<td>Configure the uplink port for the Monitor Link group</td>
<td>link-aggregation group group-id uplink</td>
<td>Required</td>
</tr>
<tr>
<td>Configure the specified link aggregation group as the uplink port of the Monitor Link group</td>
<td>smart-link group group-id uplink</td>
<td>Use any of the three approaches</td>
</tr>
<tr>
<td>Configure the specified Smart Link group as the uplink port of the Monitor Link group</td>
<td>port interface-type interface-number uplink</td>
<td></td>
</tr>
<tr>
<td>Configure the specified Ethernet port as the uplink port of the Monitor Link group</td>
<td>Monitor Link group view Ethernet port view</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a Downlink Port**

**Table 766** Configure a downlink port

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Enter the specified Monitor Link group view</td>
<td>monitor-link group group-id</td>
<td>Required</td>
</tr>
</tbody>
</table>
CHAPTER 88: MONITOR LINK CONFIGURATION

**CAUTION:**

- A Smart Link/Monitor Link group with members cannot be deleted. A Smart Link group as a Monitor Link group member cannot be deleted.
- The Smart Link/Monitor Link function and the remote port mirroring function are incompatible with each other.
- If a single port is specified as a Smart Link/Monitor Link group member, do not use the `lacp enable` command on the port or add the port to another dynamic link aggregation group because doing so will cause the port to become an aggregation group member.
- Using the copy command on a port does not copy the Smart Link/Monitor Link group member information configured on the port to any other port.

### Displaying Monitor Link Configuration

After the above-mentioned configuration, you can use the `display` command in any view to display the information about Monitor Link, so as to verify configuration result.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about one or all Monitor Link groups</td>
<td>`display monitor-link group { group-id</td>
<td>all }`</td>
</tr>
</tbody>
</table>

### Monitor Link Configuration Example

#### Implementing Collaboration Between Smart Link and Monitor Link

**Network requirements**

As shown in Figure 340, the PCs access the server and Internet through the switch. Configure Smart Link and Monitor Link to prevent the PCs from failing to access the server and Internet due to uplink link or port failure.
Network diagram

Figure 340  Network diagram for Monitor Link configuration

Configuration procedure

1. Enable Smart Link on Switch A and Switch B to implement link redundancy backup. Perform the following configuration on Switch A. The configuration on Switch B is the same as on Switch A.

   # Enter system view.

   <switchA> system-view

   # Enter Ethernet port view. Disable STP on Ethernet1/0/1 and Ethernet1/0/2.

   [SwitchA] interface Ethernet 1/0/1
   [SwitchA-Ethernet1/0/1] stp disable
   [SwitchA-Ethernet1/0/1] quit
   [SwitchA] interface Ethernet 1/0/2
   [SwitchA-Ethernet1/0/2] stp disable
   [SwitchA-Ethernet1/0/2] quit

   # Return to system view.

   [SwitchA-Ethernet1/0/2] quit

   # Create Smart Link group 1 and enter Smart Link group view.

   [SwitchA] smart-link group 1

   # Configure Ethernet 1/0/1 as the master port of the Smart Link group and Ethernet 1/0/2 as the slave port.
CHAPTER 88: MONITOR LINK CONFIGURATION

[SwitchA-smlk-group1] port Ethernet 1/0/1 master
[SwitchA-smlk-group1] port Ethernet 1/0/2 slave

# Configure to send flush messages in VLAN 1.
[SwitchA-smlk-group1] flush enable control-vlan 1

2 Enable Monitor Link on Switch C and Switch D and enable the function of processing flush messages received from VLAN 1. Perform the following configuration on Switch C. The operation procedure on Switch D is the same as that performed on Switch C.

# Enter system view.
<SwitchC> system-view

# Create Monitor Link group 1 and enter Monitor Link group view
[SwitchC] monitor-link group 1

# Configure Ethernet 1/0/1 as the uplink port of the Monitor Link group and Ethernet 1/0/2 and Ethernet 1/0/3 as the downlink ports.
[SwitchC-mtlk-group1] port Ethernet 1/0/1 uplink
[SwitchC-mtlk-group1] port Ethernet 1/0/2 downlink
[SwitchC-mtlk-group1] port Ethernet 1/0/3 downlink

# Return to system view. Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/1, Ethernet 1/0/2, and Ethernet 1/0/3.
[SwitchC-mtlk-group1] quit
[SwitchC] smart-link flush enable control-vlan 1 port Ethernet 1/0/1 to Ethernet 1/0/3

3 Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/10 and Ethernet 1/0/11 of Switch E.

# Enter system view.
<SwitchE> system-view

# Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/10 and Ethernet 1/0/11.
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 1/0/10 to Ethernet 1/0/11
Access Management Overview

Normally, client PCs in a network are connected to switches operating on the network access layer (also referred to as access switches) through Layer 2 switches; and the access switches provide external network accesses for the client PCs through their upstream links. In the network shown in Figure 341, Switch A is an access switch; Switch B is a Layer 2 switch.

**Figure 341** Typical Ethernet access networking scenario

The access management function aims to manage user access rights on access switches. It enables you to manage the external network access rights of the hosts connected to ports of an access switch.

To implement the access management function, you need to configure an IP address pool on a port of an access switch, that is, bind a specified range of IP addresses to the port.

- A port with an access management IP address pool configured only allows the hosts with their IP addresses in the access management IP address pool to access external networks.
- A port without an access management IP address pool configured allows the hosts to access external networks only if their IP addresses are not in the access management IP address pools of other ports of the switch.
Note that the IP addresses in the access management IP address pool configured on a port must be in the same network segment as the IP address of the VLAN (where the port belongs to) interface.

### Configuring Access Management

<table>
<thead>
<tr>
<th>Table 768</th>
<th>Configure access management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Enable access management function</td>
<td><code>am enable</code></td>
</tr>
<tr>
<td>Enable access management trap</td>
<td><code>am trap enable</code></td>
</tr>
<tr>
<td>Enter Ethernet port view</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>Configure the access management IP address pool of the port</td>
<td><code>am ip-pool address-list</code></td>
</tr>
<tr>
<td>Display current configuration of access management</td>
<td><code>display am [ interface-list ]</code></td>
</tr>
</tbody>
</table>

- Before configuring the access management IP address pool of a port, you need to configure the interface IP address of the VLAN to which the port belongs, and the IP addresses in the access management IP address pool of a port must be in the same network segment as the interface IP address of the VLAN which the port belongs to.

- If an access management address pool configured contains IP addresses that belong to the static ARP entries of other ports, the system prompts you to delete the corresponding static ARP entries to ensure the access management IP address pool can take effect.

- To allow only the hosts with their IP addresses in the access management address pool of a port to access external networks, do not configure static ARP entries for IP addresses not in the IP address pool.

### Access Management Configuration Examples

**Access Management Configuration Example**

**Network requirements**
Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24. The IP address of PC 2 is 202.10.20.100/24, and that of PC 3 is 202.10.20.101/24.
Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 on Switch A. The port belongs to VLAN 1, and the IP address of VLAN-interface1 is 202.10.20.200/24.

Disable the PCs that are not of Organization 1 (PC 2 and PC 3) from accessing the external network through Ethernet 1/0/1 of Switch A.

**Network diagram**

**Figure 342** Network diagram for access management configuration

![Network Diagram](image)

**Configuration procedure**

Perform the following configuration on Switch A.

```
# Enable access management.
<5500> system-view
[5500] am enable

# Set the IP address of VLAN-interface1 to 202.10.20.200/24.
[5500] interface Vlan-interface1
[5500-Vlan-interface1] ip address 202.10.20.200 24
[5500-Vlan-interface1] quit

# Configure the access management IP address pool on Ethernet 1/0/1.
[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

**Network requirements**

Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24, and those of the PCs in Organization 2 are in
the range 202.10.20.25/24 to 202.10.20.50/24 and the range 202.10.20.55 to 202.10.20.65/24.

- Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 of Switch A.
- Allow the PCs of Organization 2 to access the external network through Ethernet 1/0/2 of Switch A.
- Ethernet 1/0/1 and Ethernet 1/0/2 belong to VLAN 1. The IP address of VLAN-interface1 is 202.10.20.200/24.
- PCs of Organization 1 are isolated from those of Organization 2 on Layer 2.

**Network diagram**

**Figure 343** Network diagram for combining access management and port isolation

```
Switch A
   Eth1/0/1
   Vlan-int1 202.10.20.200/24
   Eth1/0/2
Switch B
Switch C

PC1_1 PC1_2 PC1_20
202.10.20.1/24
202.10.20.25/24
PC2_1 PC2_2 PC2_37
202.10.20.20/24
202.10.20.55/24

Organization1
Organization2
```

**Configuration procedure**

Perform the following configuration on Switch A.

For information about port isolation and the corresponding configuration, refer to the section entitled “Port Isolation Configuration” on page 181.

# Enable access management.

```
<5500> system-view
[5500] am enable
```

# Set the IP address of VLAN-interface1 to 202.10.20.200/24.

```
[5500] interface Vlan-interface 1
[5500-Vlan-interface1] ip address 202.10.20.200 24
[5500-Vlan-interface1] quit
```
# Configure the access management IP address pool on Ethernet 1/0/1.

[5500] interface Ethernet 1/0/1
[5500-Ethernet1/0/1] am ip-pool 202.10.20.1 20

# Add Ethernet 1/0/1 to the port isolation group.

[5500-Ethernet1/0/1] port isolate
[5500-Ethernet1/0/1] quit

# Configure the access management IP address pool on Ethernet 1/0/2.

[5500] interface Ethernet 1/0/2
[5500-Ethernet1/0/2] am ip-pool 202.10.20.25 26 202.10.20.55 11

# Add Ethernet 1/0/2 to the port isolation group.

[5500-Ethernet1/0/2] port isolate
[5500-Ethernet1/0/2] quit
Web authentication is a port-based authentication method that is used to control the network access rights of users. With Web authentication, users are freed from installing any special authentication client software.

With Web authentication enabled, before a user passes the Web authentication, it cannot access any network, except that it can access the authentication page or some free IP addresses. After the user passes the Web authentication, it can access any reachable networks.

Configure an ISP domain and an AAA RADIUS scheme for the domain before performing the following configurations.

**Caution:**
- Web authentication can use only a RADIUS authentication scheme; it does not support local authentication and local RADIUS authentication.
- The user number limit configured under an AAA scheme does not take effect for Web authentication. Web authentication does not support accounting. Disable accounting for the AAA scheme.

Follow the steps in Table 769 to configure Web authentication:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>Set the IP address and port number of the Web authentication server</td>
<td>web-authentication web-server</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>ip ip-address [ port port-number ]</td>
<td>If no port number is specified, port 80 will be used. No Web authentication server is set by default.</td>
</tr>
<tr>
<td>Enable Web authentication globally</td>
<td>web-authentication enable</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled globally by default</td>
</tr>
</tbody>
</table>
CHAPTER 90: WEB AUTHENTICATION CONFIGURATION

Caution:

- Before enabling global Web authentication, you should first set the IP address of a Web authentication server.
- Web authentication cannot be enabled when one of the following features is enabled, and vice versa: 802.1x, MAC authentication, port security, port aggregation and IRF.
- You can make Web authentication settings on individual ports before Web authentication is enabled globally, but they will not take effect. The Web authentication settings on ports take effect immediately once you enable Web authentication globally.
- A Web authentication client and the switch with Web authentication enabled must be able to communicate at the network layer so that the Web authentication page can be displayed on the Web authentication client.
- Web authentication is mutually exclusive with functions that depend on ACLs such as IP filtering, ARP intrusion detection, QoS, and port binding.
- After a user goes online in shared access method, if you configure an authentication-free user whose IP address and MAC address are the same as those of the online user, the online user will be forced offline.

Table 769  Configuring Web Authentication

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Web authentication on a port</td>
<td>interface interface-type</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>interface-number</td>
<td>Disabled on port by default</td>
</tr>
<tr>
<td></td>
<td>web-authentication select</td>
<td></td>
</tr>
<tr>
<td></td>
<td>method (shared</td>
<td>designated )</td>
</tr>
<tr>
<td></td>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>Set a free IP address range that can be accessed by users before Web authentication</td>
<td>web-authentication free-ip</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>ip-address { mask-length</td>
<td>mask }</td>
</tr>
<tr>
<td>Set an authentication-free user</td>
<td>web-authentication free-user</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>ip ip-address mac mac-address</td>
<td>No such user by default</td>
</tr>
<tr>
<td>Forcibly log out the specified or all users.</td>
<td>web-authentication cut</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>connection { all</td>
<td>mac mac-address</td>
</tr>
<tr>
<td></td>
<td>user-name user-name</td>
<td>interface {</td>
</tr>
<tr>
<td></td>
<td>interface-type interface-number}</td>
<td></td>
</tr>
<tr>
<td>Set the idle-user cut-down time for Web authentication</td>
<td>web-authentication timer idle-cut</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>timer</td>
<td>900 seconds by default</td>
</tr>
<tr>
<td>Set the maximum number of online Web authentication users on a port</td>
<td>web-authentication max-connection number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>number</td>
<td>128 users by default</td>
</tr>
</tbody>
</table>
Follow the steps in Table 770 to display and maintain web authentication.

### Table 770  Displaying and Maintaining Web Authentication

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display global and port Web authentication configuration information</td>
<td><code>display web-authentication configuration</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display information about specified or all online Web-authentication users.</td>
<td>`display web-authentication connection { all</td>
<td>interface { interface-type interface-number }</td>
</tr>
</tbody>
</table>

### Web Authentication Configuration Example

**Network requirements**

As shown in Figure 1-1, a user connects to the Ethernet switch through port GigabitEthernet 1/0/1.

- Configure the DHCP server so that users can obtain IP addresses from it.
- Configure Web authentication on GigabitEthernet 1/0/1 to control the access of the user to the Internet.
- Configure a free IP address range, which can be accessed by the user before it passes the Web authentication.

**Network diagram**

![Network diagram](image.png)

**Configuration procedure**

# Perform DHCP-related configuration on the DHCP server. (It is assumed that the user will automatically obtain an IP address through the DHCP server.)

# Set the IP address and port number of the Web authentication server.
<5500> system-view
[5500] web-authentication web-server ip 10.10.10.10 port 8080

# Configure a free IP address range, so that the user can access free resources before passing Web authentication.

[5500] web-authentication free-ip 10.20.20.1 24

# Enable Web authentication on GigabitEthernet 1/0/1 and set the user access method to designated.

[5500] interface GigabitEthernet 1/0/1
[5500- GigabitEthernet1/0/1] web-authentication select method designated

# Create RADIUS scheme radius1 and enter its view.

[5500] radius scheme radius1

# Set the IP address of the primary RADIUS authentication server.

[5500-radius-radius1] primary authentication 10.10.10.164

# Enable accounting optional.

[5500-radius-radius1] accounting optional

# Set the password that will be used to encrypt the messages exchanged between the switch and the RADIUS authentication server.

[5500-radius-radius1] key authentication expert

# Configure the system to strip the domain name from a user name before transmitting the user name to the RADIUS server.

[5500-radius-radius1] user-name-format without-domain
[5500-radius-radius1] quit

# Create the ISP domain aabbcc.net for Web authentication users and enter the domain view.

[5500] domain aabbcc.net

# Configure the domain aabbcc.net as the default user domain.

[5500] domain default enable aabbcc.net

# Reference scheme radius1 in domain aabbcc.net.

[5500-isp-aabbcc.net] scheme radius-scheme radius1

# Enable Web authentication globally. (3Come recommends that you perform this step last, so that valid users are prevented from accessing the network.)

[5500] web-authentication enable
Web authentication takes effect. Web authentication allows access to internal resources. To gain access to external networks (Internet), perform the following steps:

1. Enter http://10.10.10.10:8080 in the address column of IE. A page with the following prompt is displayed: Please input your name and the password!.

2. Enter the correct user name and password and then click [login]. The following page is displayed: Authentication passed!

Users can now access external networks.