3Com® Stackable Switch Family

Advanced Configuration Examples

Switch 5500
Switch 5500G
Switch 4500
Switch 4200G
Switch 4210

www.3Com.com
Part Number: 10016491 Rev. AB
Published: February 2008

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

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

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

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

Conserving energy, materials and natural resources in all operations.

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

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

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

Improving our environmental record on a continual basis.

End of Life Statement

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

Regulated Materials Statement

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

CONTENTS

About This Guide

Provides advanced configuration examples for the 3Com stackable switches, which includes the following:

- 3Com Switch 5500
- 3Com Switch 5500G
- 3Com Switch 4500
- 3Com Switch 4200G
- 3Com Switch 4210

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`

Conventions

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

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Related Documentation

The following manuals offer additional information necessary for managing your Stackable Switch. Consult the documents that apply to the switch model that you are using.

- *3Com Switch Family Command Reference Guides* — Provide detailed descriptions of command line interface (CLI) commands, that you require to manage your Stackable Switch.

- *3Com Switch Family Configuration Guides*— Describe how to configure your Stackable Switch using the supported protocols and CLI commands.
- *3Com Switch Family Quick Reference Guides* — Provide a summary of command line interface (CLI) commands that are required for you to manage your Stackable Switch .
- *3Com Stackable Switch Family Release Notes* — Contain 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 3Com World Wide Web site:

http://www.3com.com/

Products Supported by this Document

Table 2 Supported Products

Product	Orderable SKU	Description
4210	3CR17331-91	Switch 4210 9-Port
4210	3CR17332-91	Switch 4210 18-Port
4210	3CR17333-91	Switch 4210 26-Port
4210	3CR17334-91	Switch 4210 52-Port
4210	3CR17341-91	Switch 4210 PWR 9-Port
4210	3CR17342-91	Switch 4210 PWR 18-Port
4210	3CR17343-91	Switch 4210 PWR 26-Port
4500	3CR17561-91	Switch 4500 26-Port
4500	3CR17562-91	Switch 4500 50-Port
4500	3CR17571-91	Switch 4500 PWR 26-Port
4500	3CR17572-91	Switch 4500 PWR 50-Port
5500	3CR17161-91	Switch 5500-EI 28-Port
5500	3CR17162-91	Switch 5500-EI 52-Port
5500	3CR17171-91	Switch 5500-EI PWR 28-Port
5500	3CR17172-91	Switch 5500-EI PWR 52-Port
4200G	3CR17660-91	Switch 4200G 12-Port
4200G	3CR17661-91	Switch 4200G 24-Port
4200G	3CR17662-91	Switch 4200G 48-Port
4200G	3CR17671-91	Switch 4200G PWR 24-Port
5500G	3CR17250-91	Switch 5500G-EI 24 Port
5500G	3CR17251-91	Switch 5500G-EI 48-Port
5500G	3CR17252-91	Switch 5500G-EI PWR 24-Port
5500G	3CR17253-91	Switch 5500G-EI PWR 48-Port

1 DHCP CONFIGURATION EXAMPLES

Keywords:

DHCP, Option 82

Abstract:

This document describes DHCP configuration and application on Ethernet switches in specific networking environments. Based on the different roles played by the devices in the network, the functions and applications of DHCP server, DHCP relay agent, DHCP snooping, and DHCP Option 82 are covered.

Acronym:

DHCP (Dynamic Host Configuration Protocol).

Supported DHCP Functions

DHCP Functions Supported by the 3Com Stackable Switches

Table 1 DHCP functions supported by the 3Com stackable switches

Function \Model	DHCP server	DHCP relay agent	DHCP snooping
Switch 5500	●	●	●
Switch 4500	-	●	●
Switch 5500Gs	●	●	●
Switch 4200	-	-	●
Switch 4200G	-	-	●
Switch 4210	-	-	●

Depending on the models, the 3Com stackable switches can support part or all of the following DHCP functions:

The DHCP server provides the:

- Global address pool/interface address pool
- IP address lease configuration
- Allocation of subnet masks, gateway addresses, DNS server addresses, and WINS server addresses to DHCP clients
- Static bindings for special addresses
- DHCP server security functions, including detecting unauthorized DHCP servers and duplicate IP addresses

The DHCP relay agent includes the:

- DHCP relay agent
- DHCP relay agent security functions, including address checking, DHCP server handshaking, and periodic updates of client address entries

The DHCP snooping includes the:

- DHCP snooping
- DHCP snooping security functions, including DHCP snooping entry update and ARP source checking
- DHCP Snooping, Option 82

Refer to respective user manuals for detailed descriptions of the DHCP functions supported by different models.

Configuration Guide

- *This configuration varies depending on your switch's model. The example in this section uses the Switch 5500. Refer to configuration guide for your switch's model for further information. This example provides only basic configuration steps Refer to the appropriate Configuration Guide and Command Reference Guide for the function's operating principles and applications.*

Configuring the DHCP Server

The DHCP server can be configured to assign IP addresses from a global or interface address pool. These two configuration methods are applicable to the following environments:

- If the DHCP server and DHCP clients are on the same network segment, both methods can be applied.
- If the DHCP server and DHCP clients are on different network segments, the DHCP server can only be configured to assign IP addresses from a global address pool.

1 Use the following commands to configure the DHCP server to assign IP addresses from a global address pool.

Table 2 Configure IP address allocation from a global address pool

Operation	Command	Description
Enter system view	**system-view**	-
Enable the DHCP service	**dhcp enable**	Optional By default, the DHCP service is enabled.
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.
Configure an IP address range for dynamic allocation	**network** *ip-address* [*mask-length* | **mask** *mask*]	Required By default, no IP address range is configured for dynamic allocation.

Table 2 Configure IP address allocation from a global address pool

Operation			Command	Description
Configure the lease period of dynamically allocated IP addresses			**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	Optional IP address lease period defaults to one day.
Configure a domain name for DHCP clients			**domain-name** *domain-name*	Required By default, no domain name is configured for DHCP clients.
Configure DNS server addresses for DHCP clients			**dns-list** *ip-address*&<1-8>	Required By default, no DNS server addresses are configured.
Configure WINS server addresses for DHCP clients			**nbns-list** *ip-address*&<1-8>	Required By default, no WINS server addresses are configured.
Specify a NetBIOS node type for DHCP clients			**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	Optional By default, the DHCP clients are h-nodes if the command is not specified.
Configure gateway addresses for DHCP clients			**gateway-list** *ip-address*&<1-8>	Required By default, no gateway address is configured.
Configure a self-defined DHCP option			**option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	Required By default, no self-defined option is configured.
Configure a static binding	Return to system view		**quit**	Optional By default, no MAC address or client ID is bound to an IP address statically. Note: ■ To configure a static binding, you need to specify the IP address and the MAC address or client ID. ■ A static address pool can be configured with only one IP address-to-MAC or IP address-to-client ID binding.
	Create an address pool for the static address binding		**dhcp server ip-pool** *pool-name*	
	Specify the IP address of the static binding		**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*]	
	Specify the MAC address or the client ID of the static binding	Specify the MAC address of the static binding	**static-bind mac-address** *mac-address*	
		Specify the client ID of the static binding	**static-bind client-identifier** *client-identifier*	
Return to system view			**quit**	--
Specify the IP addresses to be excluded from automatic allocation			**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all the IP addresses in a DHCP address pool are available for dynamic allocation.

Table 2 Configure IP address allocation from a global address pool

Operation		Command	Description
Configure the global address pool mode	On the current interface	**interface** *VLAN-interface VLAN-interface-number*	Optional By default, an interface operates in the global address pool mode.
		dhcp select global	
		quit	
	On multiple interfaces in system view	**dhcp select global** { **interface** *VLAN-interface VLAN-interface-number* [**to** *interface-type interface-number*] | **all** }	
Enable the detection of unauthorized DHCP servers		**dhcp server detect**	Required By default, the detection of unauthorized DHCP servers is disabled.
Configure duplicate IP address detection	Set the maximum number of ping packets sent by the DHCP server for each IP address	**dhcp server ping packets** *number*	Optional The default maximum number is 2.
	Set a response timeout for each ping packet	**dhcp server ping timeout** *milliseconds*	Optional The default timeout is 500 milliseconds.
Enable the DHCP server to support Option 82		**dhcp server relay information enable**	Optional By default, the DHCP server supports Option 82.

2 Use the following commands to configure IP address allocation through the interface address pool.

Table 3 Configure IP address allocation through the interface address pool

Operation	Command	Description
Enter system view	**system-view**	-
Enable the DHCP service	**dhcp enable**	Optional By default, the DHCP service is enabled.
Configure multiple or all the VLAN interfaces to operate in interface address pool mode	**dhcp select interface** { **interface** *vlan-interface vlan-interface-number* [**to** vlan-*interface vlan-interface-number*] | **all** }	Optional

Table 3 Configure IP address allocation through the interface address pool

Operation			Command	Description
Configure a VLAN interface to operate in interface address pool mode			**interface** *interface-type interface-number* **dhcp select interface**	Required By default, a VLAN interface operates in global address pool mode.
Bind an IP address statically to a client MAC address or client ID			**dhcp server static-bind ip-address** *ip-address* { **client-identifier** *client-identifier* | **mac-address** *mac-address* }	Optional By default, no static binding is configured
Configure the lease period of dynamically allocated IP addresses	On the current interface		**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	Optional IP address lease period defaults to one day.
	On multiple interfaces in system view		**quit** **dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Return to system view			**quit**	-
Specify the IP addresses to be excluded from automatic allocation			**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all the IP addresses in an interface address pool are available for dynamic allocation.
Configure a domain name for DHCP clients		On one interface	**interface** *vlan-interface vlan-interface-number* **dhcp server domain-name** *domain-name* **quit**	Optional By default, no domain name is configured for DHCP clients.
		On multiple interfaces	**dhcp server domain-name** *domain-name* { **interface** *vlan-interface vlan-interface-number* [**to** *vlan-interface vlan-interface-number*] | **all** }	

Table 3 Configure IP address allocation through the interface address pool

Operation		Command	Description
Configure DNS server addresses for DHCP clients	On one interface	**interface** *vlan-interface vlan-interface-number*	Optional By default, no DNS server address is configured.
		dhcp server dns-list *ip-address*&<1-8>	
		quit	
	On multiple interfaces	**dhcp server dns-list** *ip-address*&<1-8> { **interface** *vlan-interface vlan-interface-number* [**to** *vlan-interface vlan-interface-number*] | **all** }	
Configure WINS server addresses for DHCP clients	On one interface	**interface** *vlan-interface vlan-interface-number*	Optional By default, no WINS server addresses are configured.
		dhcp server nbns-list *ip-address*&<1-8>	
		quit	
	On multiple interfaces	**dhcp server nbns-list** *ip-address*&<1-8> { **interface** *vlan-interface vlan-interface-number* [**to** *interface-type interface-number*] | **all** }	
Define a NetBIOS node type for DHCP clients	On one interface	**interface** *interface-type interface-number*	Optional By default, no NetBIOS node type is specified and a DHCP client uses the h-node type.
		dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }	
		quit	
	On multiple interfaces	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Table 3 Configure IP address allocation through the interface address pool

Operation		Command	Description
Configure a self-defined DHCP option	On one interface	**interface** *interface-type interface-number*	Optional By default, no self-defined option is configured.
		dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	
		quit	
	On multiple interfaces	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Enable the detection of unauthorized DHCP servers		**dhcp server detect**	Optional By default, the detection of unauthorized DHCP servers is disabled.
Configure duplicate IP address detection	Set the maximum number of ping packets sent by the DHCP server for each IP address	**dhcp server ping packets** *number*	Optional The default maximum number is 2.
	Set a response timeout for each ping packet	**dhcp server ping timeout** *milliseconds*	Optional The default timeout is 500 milliseconds.
Enable the DHCP server to support Option 82		**dhcp server relay information enable**	Optional By default, the DHCP server supports Option 82.

Configuring the DHCP Relay Agent

Use the following commands to configure the DHCP relay agent.

Table 4 Configure DHCP relay agent

Operation	Command	Description
Enter system view	**system-view**	-
Enable the DHCP service	**dhcp enable**	Optional By default, the DHCP service is enabled.
Configure DHCP server IP addresses for a DHCP server group	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	Required By default, no DHCP server IP address is configured for a DHCP server group.

Table 4 Configure DHCP relay agent

Operation	Command	Description
Configure a DHCP user address entry	**dhcp-security static** *ip-address mac-address*	Optional By default, no DHCP user address entry is configured.
Enable DHCP relay agent handshake	**dhcp relay hand enable**	Optional By default, DHCP relay agent handshake is enabled.
Configure the interval at which the DHCP relay agent updates dynamic client address entries	**dhcp-security tracker** { *interval* | **auto** }	Optional By default, the update interval is calculated automatically according to the number of the DHCP client entries.
Enable the detection on unauthorized DHCP servers	**dhcp-server detect**	Required By default, the detection of unauthorized DHCP servers is disabled.
Enable the DHCP relay agent to support Option 82	**dhcp relay information enable**	Required By default, the DHCP relay agent does not support Option 82.
Configure a strategy for the DHCP relay agent to handle request packets containing Option 82	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Optional By default, the strategy is **replace**.
Enter VLAN interface view	**interface** *interface-type interface-number*	-
Associate the interface to a DHCP server group	**dhcp-server** *groupNo*	Required By default, a VLAN interface is not associated to any DHCP server group.
Enable the address checking function for the DHCP relay agent	**address-check enable**	Required By default, the address checking function is disabled for the DHCP relay agent.

Configuring DHCP Snooping

Use the following commands to configure DHCP snooping:

Table 5 Configure DHCP snooping

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP snooping	**dhcp-snooping**	Required By default, DHCP snooping is disabled.
Enter Ethernet port view	**interface eth\gig-***interface-type unit/0/0port-number*	-
Specify the port connected to the DHCP server as a trusted port	**dhcp-snooping trust**	Optional By default, all the ports of a switch are untrusted ports.

DHCP Server Configuration Example

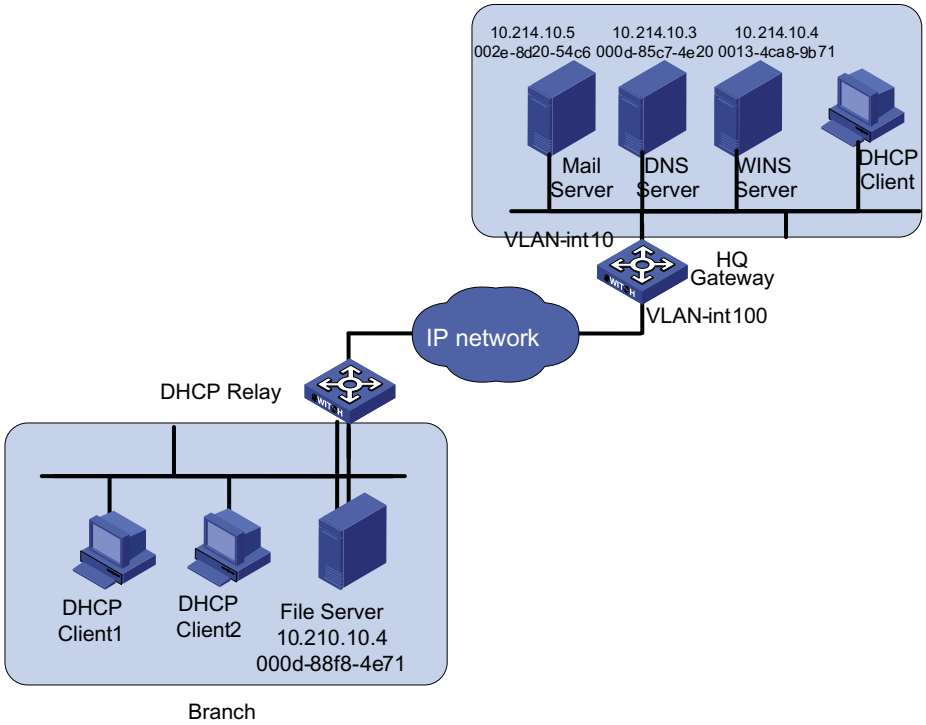
Network Requirements

A Switch 5500 serves as the DHCP server in the corporate headquarters (HQ) to allocate IP addresses to the workstations in the HQ and a branch, and it also acts as the gateway to forward packets from the HQ. The network requirements are as follows:

- Assign the HQ the IP addresses in the 10.214.10.0/24 network segment, with a lease period of two days, and exclude the IP addresses of the DNS server, WINS server, and mail server from allocation.
- Assign IP addresses to the DNS server, WINS server, and the mail server in HQ through static bindings.
- Assign the workstations in the Branch the IP addresses in the 10.210.10.0/24 network segment, with a lease period of three days, and assign the file server in the Branch an IP address through a static IP-to-MAC binding.
- Assign the addresses of the gateway, DNS server, and the WINS server along with an IP address to each workstation in the HQ and Branch.
- Enable the detection of unauthorized DHCP servers to prevent any unauthorized DHCP server from allocating invalid addresses.

Network Diagram

Figure 1 Network diagram for DHCP server configuration



Configuration Procedure

Software Version Used

This example uses the Switch 5500 running software version 3.2.

Configuring DHCP server

- Configure address allocation for the devices in the HQ.

Configure the IP address of VLAN-interface10 on the DHCP server in the HQ.

```
<3Com> system-view
[3Com] interface Vlan-interface 10
[3Com-Vlan-interface10] ip address 10.214.10.1 24
```

Configure the interface to operate in the interface address pool mode, assigning the IP addresses in the 10.214.10.0/24 network segment to the devices in the HQ.

```
[3Com-Vlan-interface10] dhcp select interface
```

Configure the address lease period of the address pool, and configure the IP addresses of the DNS server and WINS server.

```
[3Com-Vlan-interface10] dhcp server expired day 2
[3Com-Vlan-interface10] dhcp server dns-list 10.214.10.3
[3Com-Vlan-interface10] dhcp server nbst-list 10.214.10.4
```

No gateway needs to be configured for the clients because an interface operating in the interface address pool mode automatically serves as the gateway for DHCP clients and sends the requested information to the clients.

Assign IP addresses to the DNS server, WINS server, and mail server through IP-to-MAC bindings.

```
[3Com-Vlan-interface10] dhcp server static-bind ip-address 10.214.10
.3 mac-address 000d-85c7-4e20
[3Com-Vlan-interface10] dhcp server static-bind ip-address 10.214.10
.4 mac-address 0013-4ca8-9b71
[3Com-Vlan-interface10] dhcp server static-bind ip-address 10.214.10
.5 mac-address 002e08d20-54c6
```

Exclude the static IP addresses of the DNS server, WINS server, and mail server from allocation.

```
[3Com-Vlan-interface10] quit
[3Com] dhcp server forbidden-ip 10.214.10.3 10.214.10.5
```

- Configure address allocation for the devices in the Branch.

Create a global address pool named “br” for the Branch, and specify the range and lease period of the IP addresses for allocation.

```
[3Com] dhcp server ip-pool br
[3Com-dhcp-pool-br] network 10.210.10.0 mask 255.255.255.0
[3Com-dhcp-pool-br] expired day 3
```

Create a static binding address pool named “br-static”, and assign the file server in the Branch an IP address through an IP-to-MAC binding.

```
[3Com-dhcp-pool-br] quit
[3Com] dhcp server ip-pool br-static
[3Com-dhcp-pool-br-static] static-bind ip-address 10.214.10.4 mask 2
55.255.255.0
[3Com-dhcp-pool-br-static] static-bind mac-address 000d-88f8-4e71
```

Specify the gateway address, DNS server address, and the WINS server address for the workstations in the Branch.

```
[3Com-dhcp-pool-br-static] quit
[3Com] dhcp server ip-pool br
[3Com-dhcp-pool-br] gateway-list 10.210.10.1
[3Com-dhcp-pool-br] dns-list 10.214.10.3
[3Com-dhcp-pool-br] nbst-list 10.214.10.4
```

Exclude the static IP address of the gateway in the Branch from allocation.

```
[3Com-dhcp-pool-br] quit
[3Com] dhcp server forbidden-ip 10.210.10.1
```

Enable the detection of unauthorized DHCP servers.

```
[3Com] dhcp server detect
```

Configure VLAN-interface100 to operate in the global address pool mode.

```
[3Com] interface Vlan-interface 100
[3Com-Vlan-interface100] dhcp select global
```

Note that:

After DHCP configuration is complete, IP addresses can be assigned to the workstations in the Branch only when a route is active between the HQ and the Branch.

Configuring the DHCP relay agent

This section mainly describes the DHCP server configuration. The following shows the basic DHCP relay agent configuration that ensures the DHCP relay agent to relay DHCP requests to the DHCP server. For details about DHCP relay agent configuration, see "DHCP Relay Agent/Snooping Configuration Examples" on page 19.

```
<3Com> system-view
[3Com] dhcp-server 1 ip 10.214.10.1
[3Com] interface Vlan-interface 5 (define Vlan 5 in configuration
above)
[3Com-Vlan-interface5] dhcp-server 1
```

DHCP Relay Agent/Snooping Configuration Examples

Network Requirements

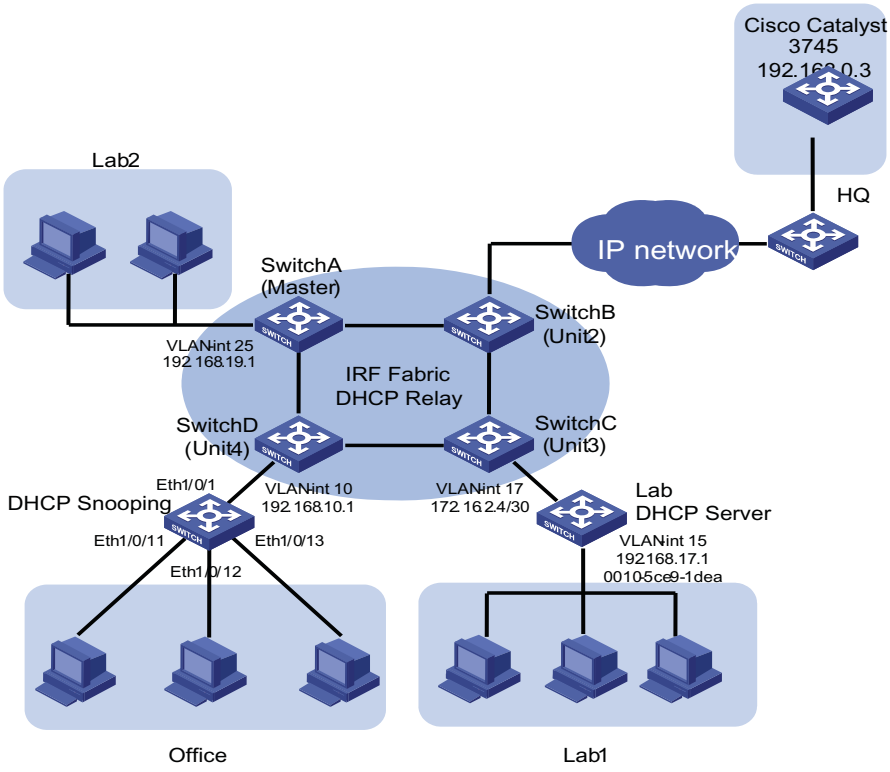
A Cisco Catalyst 3745 switch is deployed in the HQ and serves as the DHCP server to assign IP addresses to the workstations in the Office branch. The branches are

connected to an XRN (Expandable resilient network) Fabric that serves as the central node and the DHCP relay agent to forward the DHCP requests from the workstations. Meanwhile, a lab DHCP server is used to assign IP addresses to the devices in the labs. The network requirements are as follows:

- Configure the DHCP server in the HQ to assign the IP addresses in the 192.168.10.0/24 network segment to the workstations in the Office branch, with a lease period of 12 hours. Configure the IP addresses of the DNS server and WINS server as 192.169.100.2 and 192.168.100.3 respectively.
- The XRN Fabric is connected to the branches and is comprised of four switches. It serves as the DHCP relay agent to forward the DHCP requests from the workstations in the Office and the devices in the labs. It is enabled to detect unauthorized DHCP servers.
- An Ethernet switch in Lab1 serves as the Lab DHCP server to assign the IP addresses in the 192.168.17.0/24 network segment to the devices in Lab1, with a lease period of one day, and to assign the IP addresses in the 192.168.19.0/24 network segment to Lab2, with a lease period of two days. The lab DHCP server and the XRN Fabric are interconnected through the 172.16.2.4/30 network segment.
- Configure the address checking function on the DHCP relay agent so that only the devices that are assigned legal IP addresses from the DHCP server are allowed to access the external network.
- Configure address entry update on the DHCP relay agent so that it updates the address entries by sending requests to the DHCP server every one minute.
- Enable DHCP snooping to support DHCP Option 82, adding local port information to the Option 82 field in DHCP messages.
- Enable the DHCP relay agent to support DHCP Option 82 so that the DHCP relay agent keeps the original filed unchanged upon receiving DHCP messages carrying Option 82.
- Enable the DHCP server to support DHCP Option 82 so that it assigns the IP addresses 192.168.10.2 through 192.168.10.25 to the DHCP clients connected to Ethernet1/0/11 on the DHCP snooping switch and assigns 192.168.10.100 through 192.168.10.150 to the DHCP clients connected to Ethernet1/0/12 of the DHCP snooping switch.

Network Diagram

Figure 2 Network diagram for DHCP relay agent/snooping integrated configuration



Configuration Procedure

In this example, the XRN Fabric is comprised of Switch 5500s running software version 3.2, a Switch 7750 switch running software version Release 0028 is used as the DHCP snooping-capable switch, and a 3Com Switch 7750 Family S3528 switch running software version Release 0028 is used as the Lab DHCP server.

For better readability:

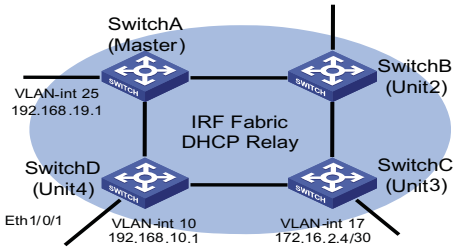
- The devices in the XRN Fabric are SwitchA, SwitchB, SwitchC, and SwitchD.
- The DHCP snooping-capable device is referred to as "Snooping".
- The device serving as the Lab DHCP server is referred to as "LAB".

Configuring XRN Fabric

The Switch 5500 supports XRN Fabric. You can interconnect four devices to form a Fabric for centralized management of the devices in the Fabric. For details, see the related sections in the *Switch 5500 Family Configuration Guide*.

Configuring the DHCP relay agent

Figure 3 Network diagram for DHCP relay agent configuration



Within the XRN Fabric, configuration made on a device can be synchronized to the other devices. Therefore, configuration is performed on Switch A only in this example.

Configure to forward the DHCP requests from the Office to the DHCP server in the HQ.

```
<SwitchA> system-view
[SwitchA] dhcp-server 1 ip 192.168.0.3
[SwitchA] interface vlan-interface10
[SwitchA-Vlan-interface10] ip address 192.168.10.1 24
[SwitchA-Vlan-interface10] dhcp-server 1
```

Configure to forward the DHCP requests from Lab2 to the Lab DHCP server.

```
[SwitchA-Vlan-interface10] quit
[SwitchA] dhcp-server 2 ip 192.168.17.1
[SwitchA] interface Vlan-interface 25
[SwitchA-Vlan-interface25] ip address 192.168.19.1 24
[SwitchA-Vlan-interface25] dhcp-server 2
```

Configure the IP address of VLAN-interface17 as 172.16.2.5/30 for forwarding DHCP packets from the Lab DHCP Server to a non-local segment.

```
[SwitchA-Vlan-interface25] quit
[SwitchA] interface Vlan-interface 17
[SwitchA-Vlan-interface17] ip add 172.16.2.5 30
```

Configure the address checking function on the DHCP relay agent. Make sure you configure the IP addresses and MAC addresses of the two DHCP servers as static entries for the security function.

```
[SwitchA-Vlan-interface17] quit
[SwitchA] dhcp-security static 192.168.0.3 000D-88F8-4E71
[SwitchA] dhcp-security static 192.168.17.1 0010-5ce9-1dea
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] address-check enable
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 25
[SwitchA-Vlan-interface25] address-check enable
[SwitchA-Vlan-interface25] quit
```

Configure the address entry update interval on the DHCP relay agent.

```
[SwitchA] dhcp relay hand enable
[SwitchA] dhcp-security tracker 60
```

Enable the DHCP relay agent to support DHCP Option 82 and adopt the strategy of keeping the original filed upon receiving DHCP messages carrying Option 82.

```
[SwitchA] dhcp relay information enable
[SwitchA] dhcp relay information strategy keep
```

Enable the DHCP relay agent to detect unauthorized DHCP servers.

```
[SwitchA] dhcp-server detect
```

Enable UDP-Helper so that the XRN Fabric can operate in the DHCP relay agent mode.

```
[SwitchA] udp-helper enable
```

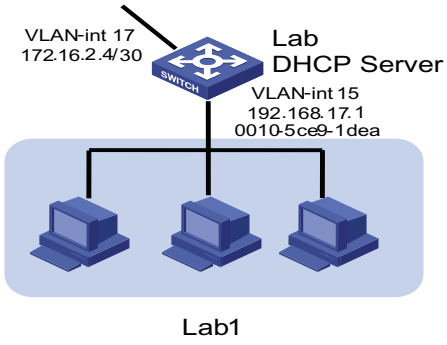
To ensure normal forwarding of DHCP packets across network segments, you need configure a routing protocol and advertise the network segments of interfaces. The following configuration uses RIP as an example. For the configuration of other routing protocols, see the parts covering routing protocols in product manuals.

```
[SwitchA] rip
[SwitchA-rip] network 192.168.10.0
[SwitchA-rip] network 192.168.19.0
[SwitchA-rip] network 172.16.0.0
```

For the DHCP relay agent using the XRN structure and the DHCP server in the HQ to communicate with each other, an active route must also be configured between them. This configuration is performed by the ISP or the user; therefore, it will not be covered in this document.

Configuring the Lab DHCP server

Figure 4 Network diagram for the Lab DHCP server configuration



Configure an address pool for Lab2 and specify the address range, lease period, and the gateway address.

```
<LAB> system-view
[LAB] dhcp enable
[LAB] dhcp server ip-pool lab2
[LAB-dhcp-lab2] network 192.168.19.0 255.255.255.0
[LAB-dhcp-lab2] expired day 2
[LAB-dhcp-lab2] gateway-list 192.168.19.1
```

Configure the IP address of VLAN-interface17 as 172.16.2.6/30 and enable it to operate in global address pool mode.

```
[LAB-dhcp-lab2] quit
[LAB] interface Vlan-interface 17
[LAB-Vlan-interface17] ip address 172.16.2.6 30
[LAB-Vlan-interface17] dhcp select global
```

Lab1 is connected to VLAN-interface15. Therefore, to assign the IP addresses in the 192.168.17.0/24 network segment to the devices in Lab1, you only need to configure VLAN-interface15 to operate in the interface address pool mode.

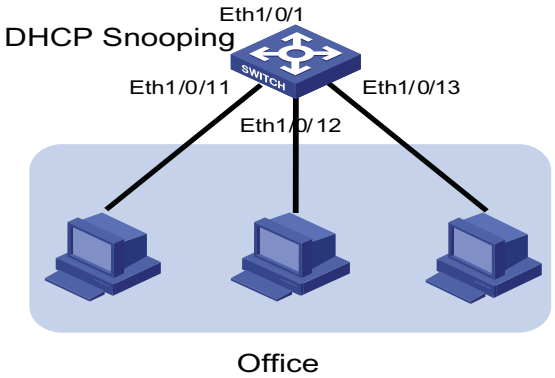
```
[LAB-Vlan-interface17] quit
[LAB] interface vlan-interface 15
[LAB-Vlan-interface15] ip address 192.168.17.1 24
[LAB-Vlan-interface15] dhcp select interface
[LAB-Vlan-interface15] quit
```

To ensure that the lab DHCP server forwards DHCP packets normally, you need configure a routing protocol. The following configuration uses RIP as an example. For the configuration of other routing protocols, see the related parts in product manuals.

```
[LAB] rip
[LAB-rip] network 192.168.17.0
[LAB-rip] network 172.16.0.0
```

Configuring DHCP snooping

Figure 5 Network diagram for DHCP snooping configuration



Enable DHCP snooping and enable Option 82 support for DHCP snooping.

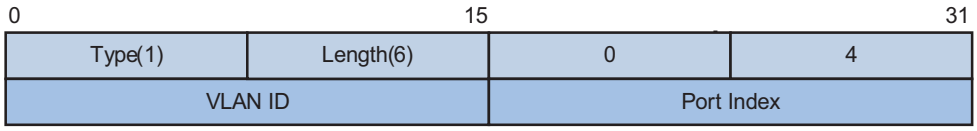
```
<Snooping> system-view
[Snooping] dhcp-snooping
[Snooping] dhcp-snooping information enable
[Snooping] dhcp-packet redirect Ethernet 0/11 to 0/13
```

Configuring the DHCP server in the HQ

On the 3Com series switches, port numbers, VLAN numbers, and the MAC addresses of the DHCP snooping device and the DHCP relay agent are added to DHCP Option 82. A complete piece of Option 82 information is a combination of the values of two suboptions:

Circuit ID suboption: It identifies the VLAN to which the clients belong and the port to which the DHCP snooping device is connected.

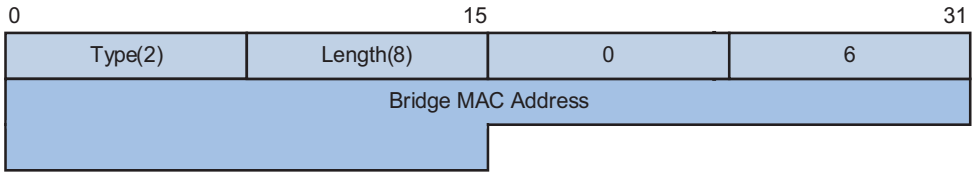
Figure 6 Packet structure of Circuit ID suboption



For example, the DHCP messages from clients connected to Ethernet1/0/11 are added with Option 82, whose Circuit ID suboption should be 0x010600040001000a, where 01060004 is a fixed value, 0001 indicates the access port's VLAN is VLAN 1, and 000a is the absolute number of the port, which is 1 less than the actual port number, indicating the actual port is Ethernet1/0/11.

Remote ID suboption: It identifies the MAC address of the DHCP snooping device connected to the client.

Figure 7 Packet structure of Remote ID suboption



For example, the DHCP messages from clients connected to the DHCP snooping device with MAC 000f-e234-bc66 are added with Option 82, whose Remote ID suboption should be 02080006000fe234bc66, where 02080006 is a fixed value and 000fe234bc66 is the MAC address of the DHCP snooping device.

In this example, IP addresses are assigned based on port number only. Therefore, on the DHCP server, only a matching port number field in the Circuit ID suboption needs to be found.

The following configuration is performed on the Cisco Catalyst 3745 switch running IOS version 12.3(11)T2. If you are using any other models or devices running any other version, see the user manuals provided with the devices.

Enable DHCP server and allocate IP addresses using Option 82 information.

```
Switch> enable
Switch(config)# configure terminal
Enter Configuration commands, one per line. End with CNTL/Z.
Switch(config)# service dhcp
Switch(config)# ip dhcp use class
```

Create a DHCP class for the client connected to Ethernet1/0/11 of the DHCP snooping device and match the port number in the Circuit ID suboption of Option82, and replace the contents without match need with a wildcard "*".

```
Switch(config)# ip dhcp class office1
Switch(dhcp-class)# relay agent information hex 010600040001000a*
Switch(dhcp-class)# exit
```

Configure a DHCP class for the client connected to Etherent1/0/12 of the DHCP snooping device and match the port number in the Circuit ID suboption of Option82.

```
Switch(config)# ip dhcp class office2
Switch(dhcp-class)# relay agent information hex 010600040001000b*
```

Create an address pool for Office and specify address ranges for the two DHCP classes.

```
Switch(config)# ip dhcp pool office
Switch(dhcp-pool)# network 192.168.10.0
Switch(dhcp-pool)# class office1
Switch(dhcp-pool-class)# address range 192.168.10.2 192.168.10.25
Switch(dhcp-pool-class)# exit
Switch(dhcp-pool)# class office2
Switch(dhcp-pool-class)# address range 192.168.10.100 192.168.10.150
Switch(dhcp-pool-class)# exit
```

Configure the lease period, gateway address, DNS server address, and WINS server address for the address pool.

```
Switch(dhcp-pool)# lease 0 12
Switch(dhcp-pool)# default-router 192.168.10.1
Switch(dhcp-pool)# dns-server 192.168.100.2
Switch(dhcp-pool)# netbios-name-server 192.168.100.3
```

After the above-mentioned configuration, the DHCP server can automatically assign an IP address, the gateway address, DNS server address, and the WINS server address for each device in Office.

Precautions

Cooperation Between DHCP Relay Agent and XRN

- In an XRN network, the DHCP relay agent runs on all the units in the Fabric. But only the DHCP relay agent running on the master unit can receive and send packets to perform full DHCP relay agent functions. The DHCP relay agent running on a slave unit, however, only serves as a backup for the master unit.
- DHCP is an application-layer protocol based on UDP. Once a slave unit receives a DHCP request, UDP-Helper redirects the packet to the master unit. Then, the DHCP relay agent running on the master unit gives a response back to the

request and sends the real time information to each slave unit for backup. In this way, when the current master unit fails, one of the slaves becomes the new master and operates as the DHCP relay agent immediately. Therefore, make sure you enable UDP-Helper before using DHCP relay agent in an XRN system.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

2 QACL CONFIGURATION EXAMPLES

Key words:

ACL, and QoS

Abstract:

This document describes QACL configurations on Ethernet switches in actual networking environments. To satisfy different user needs, the document covers various functions and applications like time-based ACLs, traffic policing, priority re-marking, queue scheduling, traffic measurement, port redirection, local traffic mirroring, and WEB Cache redirection.

Acronyms:

Access control list (ACL), and quality of service (QoS)

Supported QACL Functions

ACL/QoS Functions Supported by 3Com Stackable Switches

Table 6 ACL/QoS functions supported by 3Com stackable switches

Function\Model	Switch 5500	Switch 4500	Switch 5500G	Switch 4200G	Switch 4210
Basic ACL	●	●	●	●	●
Advanced ACL	●	●	●	●	●
Layer 2 ACL	●	●	●	-	-
User-defined ACL	●	●	●	-	-
Software-based ACL referenced by upper-layer software	●	●	●	●	●
Apply hardware-based ACL to hardware	●	●	●	-	-
Traffic classification	●	●	●	-	-
Priority re-marking	●	●	●	-	-
Port rate limiting	●	●	●	●	●
Traffic policing	●	●	●	-	-
Traffic shaping	-	-	-	-	-
Port redirection	●	●	●	-	-

Table 6 ACL/QoS functions supported by 3Com stackable switches

Function\Model	Switch 5500	Switch 4500	Switch 5500G	Switch 4200G	Switch 4210
Queue scheduling	●	●	●	●	●
Congestion avoidance	●	●	-	-	-
Local traffic mirroring	●	●	●	-	-
Traffic measurement	●	●	●	-	-
WEB Cache redirection	●	-	-	-	-

● *means that the function is supported.*

- means that the function is not supported.

For details on the ACL and QoS functions supported by different models, refer to switch model's configuration guide.

Configuration Guide

- *ACL/QoS configuration varies with switch models. The configuration below uses a 3Com Switch 5500 as an example. For ACL/QoS configuration on other switches, refer to corresponding user manuals.*
- *The section below lists basic configuration steps. For the function's detailed operational instructions, refer to the configuration guide and command reference guidecommand reference guide for the applicable product.*

Table 7 Configure ACL/QoS in system view

Configuration	Command	Remarks
Create an ACL and enter ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	By default, the matching order is **config**. Layer 2 ACLs and user-defined ACLs do not support **match-order**.
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	The parameters (criteria) available for *rule-string* vary with ACL types. For additional details, refer to the corresponding command reference guide.

Table 7 Configure ACL/QoS in system view

Configuration	Command	Remarks
Configure a queue scheduling algorithm in system view	**queue-scheduler** { **strict-priority** | **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	■ If the weight or minimum bandwidth of a queue is set to 0 in the WRR or WFQ approach, strict priority queuing applies to the queue. ■ By default, the WRR queue scheduling algorithm is used for all outbound queues on a port. Default weights are 1:2:3:4:5:9:13:15. ■ The queue scheduling algorithm defined using the **queue-scheduler** command in system view will work on all ports.
Configure congestion avoidance	**wred** *queue-index qstart probability*	-

Table 8 Configure ACL/QoS in port view

Configuration	Command	Remarks
Apply an ACL on a port	**packet-filter** { **inbound** | **outbound** } *acl-rule*	-
Configure the switch to trust the priority of received packets	**priority trust**	Configure the switch to trust the priority carried in received packets.
Configure port-based rate limit	**line-rate** { **inbound** | **outbound** } *target-rate*	The granularity is 64 kbps. If an entered number is in the range N×64 to (N+1)×64 (N is a natural number), the switch takes the value (N+1)×64.
Reference an ACL for traffic identification, and re-assign a priority to the matching packets	**traffic-priority** { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	You can re-mark the IP priority, 802.1p priority, DSCP priority of packets, and the priority of local queues.
Configure traffic policing	**traffic-limit inbound** *acl-rule target-rate* [**exceed** *action*]	**exceed** *action*: specifies the action taken on the excess packets when the packet traffic exceeds the preset limit. ■ **drop**: Drop the excess packets. ■ **remark-dscp** *value*: Re-set the DSCP priority, and forward the packets.

Table 8 Configure ACL/QoS in port view

Configuration	Command	Remarks
Configure a queue scheduling algorithm in port view	**queue-scheduler** { **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	■ The queue scheduling algorithm defined using the **queue-scheduler** command in Ethernet port view will work on the current port only. ■ In the globally defined WRR or WFQ queue scheduling algorithm, you can modify the weight or bandwidth in port view if the weight or bandwidth of each queue cannot satisfy the needs of a port. ■ Queue weight or bandwidth defined in port view take priority over the global settings. ■ The queue weight or bandwidth defined in port view cannot be displayed using the **display queue-scheduler** command.
Configure redirection	**traffic-redirect** { **inbound** | **outbound** } *acl-rule* { **cpu** | **interface** *interface-type interface-number* }	A packet cannot be forwarded normally if it is redirected to the CPU.
Reference an ACL for traffic identification, and measure the traffic of the matching packets	**traffic-statistic inbound** *acl-rule*	-

Network Environment

Figure 8 Network topology

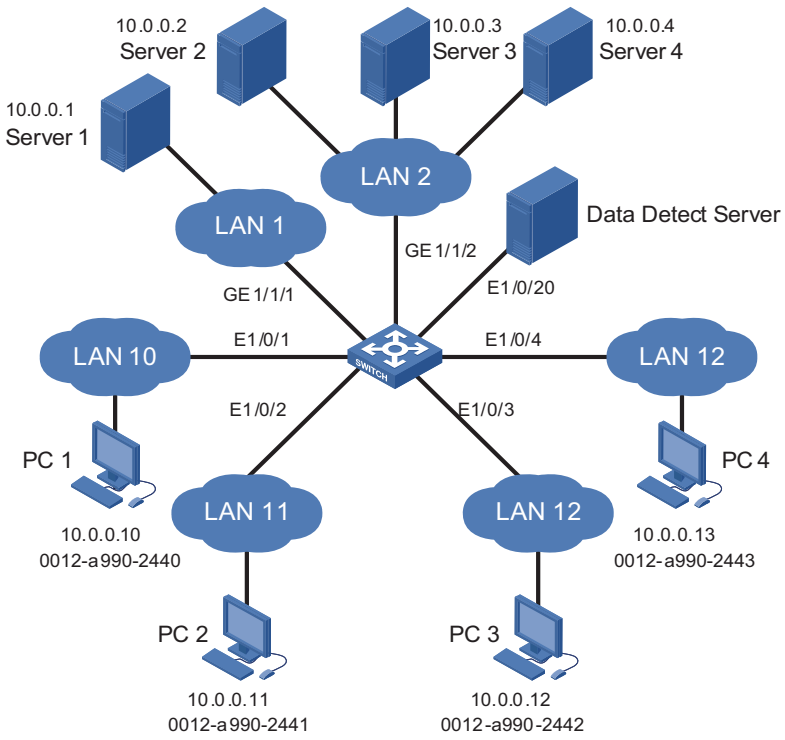


Figure 8 shows the network topology of a company. The environment is as follows:

- A Switch 5500 serves as the central switch of the company. The software version is Release 3.2.
- The devices within the company gain access to the Internet through Server1 attached to the port GigabitEthernet1/1/1.
- Server2, Server3, and Server4 are the data server, mail server and file server of the company respectively. They are connected to the port GigabitEthernet1/1/2.
- The Data Detect Server is connected to the port Ethernet1/0/20.
- PC1, PC2, PC3 and PC4 are clients of the company, and are connected to the ports Ethernet1/0/1, Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 respectively.

Time-based ACL plus Rate Limiting plus Traffic Policing Configuration Example

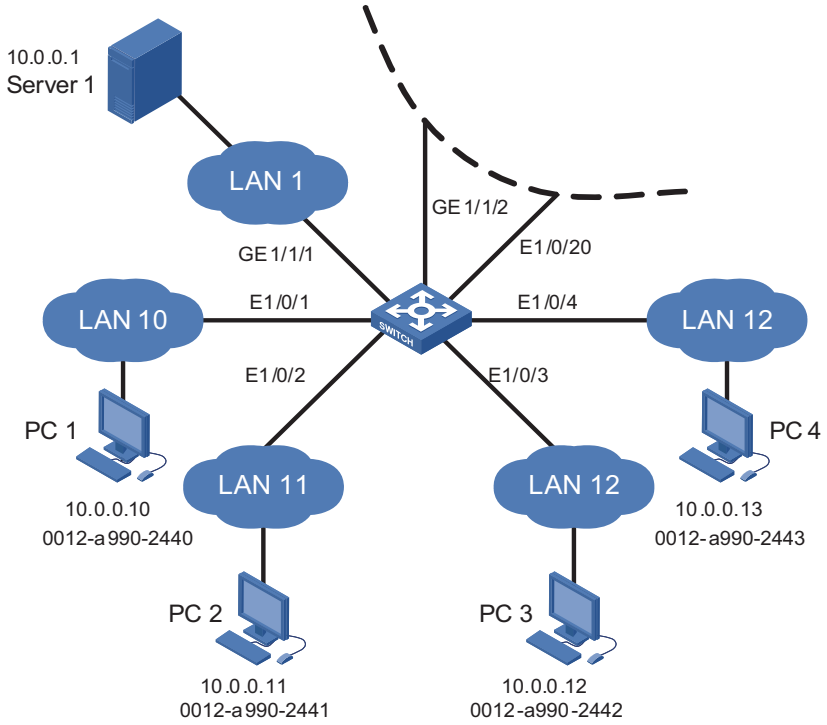
Network Requirements

The company gains access to the Internet through Server1. The requirements are as follows:

- During the period from 8:30 to 18:30 in workdays, the clients are not allowed to access the Internet through HTTP. In other periods, the clients are allowed to access the Internet. The maximum access traffic is 100 Mbps.
- For the packets with the IP priority of 7 that are sent by PC 1, the allowed maximum rate is 20 Mbps. The DSCP priority of such packets at rates higher than 20 Mbps is modified as EF.
- For the packets with the CoS priority of 5 that are sent by PC 2, the allowed maximum rate is 10 Mbps. Such packets at rates higher than 10 Mbps are discarded.

Network Diagram

Figure 9 Network diagram for configuration of time-based ACL plus port-based bandwidth limiting plus traffic policing



Configuration Procedure

Create time range a001, defining the office hours on working days.

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] time-range a001 8:30 to 18:00 working-day
```

Create time range a002, defining off hours.

```
[3Com] time-range a002 00:00 to 8:30 working-day
[3Com] time-range a002 18:00 to 24:00 working-day
[3Com] time-range a002 00:00 to 24:00 off-day
```

Define ACL 3010: Forbid the clients to access the Internet through HTTP during the time range a001; classify and mark the packets with the IP priority of 7 generated when PC 1 accesses the Internet during non-workday periods.

```
[3Com] acl number 3010
[3Com-acl-adv-3010] rule 0 deny tcp destination 10.0.0.1 0 destinati
```

```
on-port eq 80 time-range a001
[3Com-acl-adv-3010] rule 1 permit ip source 10.0.0.10 0 precedence 7
 time-range a002
[3Com-acl-adv-3010] quit
```

Define ACL 4010: Classify and mark the packets with the CoS priority of 5 generated when PC 2 accesses the Internet during non-work periods.

```
[3Com] acl number 4010
[3Com-acl-ethernetframe-4010] rule 0 permit cos 5 source 0012-0990-2
241 ffff-ffff-ffff time-range a002
[3Com-acl-ethernetframe-4010] quit
```

Apply rule 0 of ACL 3010 to the port GigabitEthernet1/1/1 connected to Server1, and set the maximum traffic rate by clients' accessing the Internet to 100 Mbps.

```
[3Com] interface GigabitEthernet 1/1/1
[3Com-GigabitEthernet1/1/1] packet-filter outbound ip-group 3010 rule 0
[3Com-GigabitEthernet1/1/1] line-rate outbound 102400
[3Com-GigabitEthernet1/1/1] quit
```

Perform traffic policing for the packets marked rule 1 of ACL 3010 on the port Ethernet1/0/1 connected to PC 1, and modify the DSCP priority of the excess packets to EF.

```
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/1] traffic-limit inbound ip-group 3010 rule 1 2048
0 exceed remark-dscp ef
[3Com-Ethernet1/0/1] quit
```

Perform traffic policing for the packets marked rule 0 of ACL 4010 on the port Ethernet1/0/2 connected to PC 2, set the maximum traffic rate to 10 Mbps, and discard the excess packets.

```
[3Com] interface Ethernet 1/0/2
[3Com-Ethernet1/0/2] traffic-limit inbound link-group 4010 rule 0 10
240 exceed drop
```

*The **traffic-limit** command works only with the **permit** rules in ACLs.*

Configuration Example of Priority Re-marking plus Queue Scheduling Algorithm plus Congestion Avoidance plus Packet Priority Trust

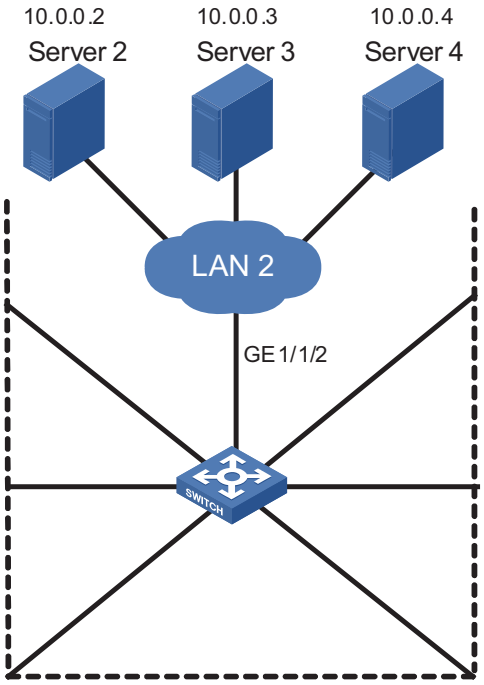
Network Requirements

Server2, Server3, and Server4 are the data server, mail server and file server of the company respectively. The detailed requirements are as follows:

- The switch first processes the packets accessing the data server, then the packets accessing the mail server, and finally the packet accessing the file server.
- Configure the port GigabitEthernet1/1/2 to use the WRR queue priority algorithm, and configure the weight of outbound queues as 1:1:1:5:1:10:1:15.
- Configure the queue with an index of 4 on the port GigabitEthernet1/1/2 to use WRED: Discard subsequent packets at random when the queue is more than 64 packets in size, and configure the probability of discarding as 20%.
- Configure the port Ethernet1/0/3 to trust the priority of packets rather than to use the priority of the port.

Network Diagram

Figure 10 Network diagram for configuration of priority re-marking plus queue scheduling algorithm plus congestion avoidance plus packet priority trust



Configuration Procedure

Define ACL 3020: Classify and mark packets according to their destination IP addresses.

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] acl number 3020
[3Com-acl-adv-3020] rule 0 permit ip destination 10.0.0.2 0
[3Com-acl-adv-3020] rule 1 permit ip destination 10.0.0.3 0
[3Com-acl-adv-3020] rule 2 permit ip destination 10.0.0.4 0
[3Com-acl-adv-3020] quit
```

Re-mark priority for the packets on the port GigabitEthernet1/1/2 that match the rules in ACL 3020.

```
[3Com] interface GigabitEthernet 1/1/2
[3Com-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020
rule 0 local-precedence 7
```

```
[3Com-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020
rule 1 local-precedence 5
[3Com-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020
rule 2 local-precedence 3
```

Configure the WRR queue scheduling algorithm on the port GigabitEthernet1/1/2, and configure the weight of outbound queues as 1:1:1:5:1:10:1:15.

```
[3Com-GigabitEthernet1/1/2] queue-scheduler wrr 1 1 1 5 1 10 1 15
```

Configure the queue with an index of 4 on the port GigabitEthernet1/1/2 to use WRED: Discard subsequent packets at random when the queue is more than 64 packets in size, and configure the probability of discarding as 20%.

```
[3Com-GigabitEthernet1/1/2] wred 4 64 20
[3Com-GigabitEthernet1/1/2] quit
```

Configure the port Ethernet1/0/3 connected to PC 3 to trust the 802.1p priority carried by packets.

```
[3Com] interface Ethernet 1/0/3
[3Com-Ethernet1/0/3] priority trust
```

*The **traffic-priority** command works only with the **permit** rules in ACLs.*

Configuration Example of Traffic Measurement plus Port Redirection

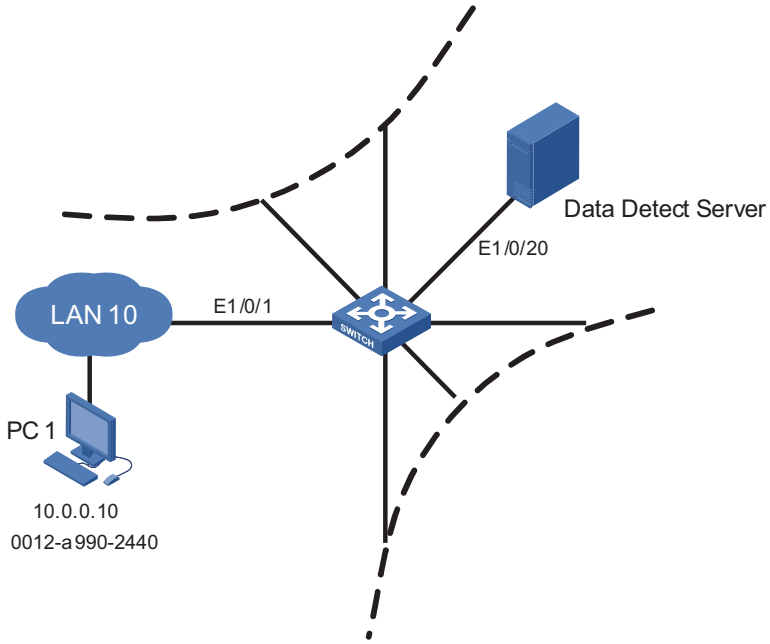
Network Requirements

The Data Detect Server is connected to the port Ethernet1/0/20. The detailed requirements are as follows:

- Measure the HTTP traffic generated by Internet access through the port Ethernet1/0/1 during non-workday periods.
- Redirect all the HTTP traffic generated by the Internet access through the port Ethernet1/0/1 during workday period to the port Ethernet1/0/20.

Network Diagram

Figure 11 Network diagram for configuration of traffic measurement plus port redirection



Configuration Procedure

Configure a workday period.

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] time-range a001 8:30 to 18:00 working-day
```

Configure non-workday periods.

```
[3Com] time-range a002 00:00 to 8:30 working-day
[3Com] time-range a002 18:00 to 24:00 working-day
[3Com] time-range a002 00:00 to 24:00 off-day
```

Define ACL 3030: Classify the packets accessing the Internet through HTTP according to periods.

```
[3Com] acl number 3030
[3Com-acl-adv-3030] rule 0 permit tcp destination 10.0.0.1 0 destina
tion-port eq 80 time-range a001
[3Com-acl-adv-3030] rule 1 permit tcp destination 10.0.0.1 0 destina
tion-port eq 80 time-range a002
```

Configure traffic redirection on the port Ethernet1/0/1: Redirect all the HTTP traffic generated by Internet access during workday period to the port Ethernet1/0/20.

```
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/1] traffic-redirect inbound ip 3030 rule 0 interfa
ce Ethernet 1/0/20
```

Measure the HTTP traffic generated by Internet access during non-workday periods on the port Ethernet1/0/1.

```
[3Com-Ethernet1/0/1] traffic-statistic inbound ip-group 3030 rule 1
```

*The **traffic-redirect** and **traffic-statistic** commands work only with the **permit** rules in ACLs.*

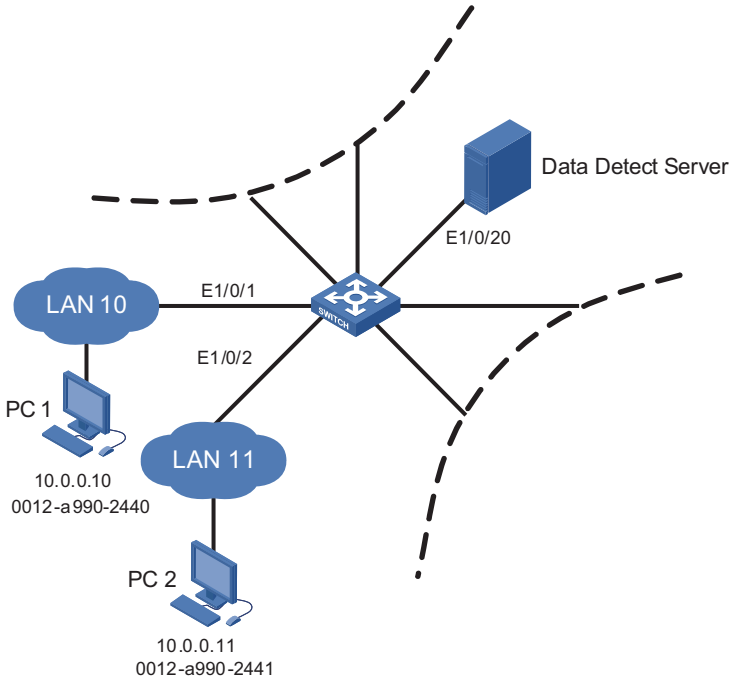
Configuration Example of Local Traffic Mirroring

Network Requirements

The Data Detect Server is connected to the port Ethernet1/0/20. All the packets accessing the Internet through the ports Ethernet1/0/1 and Ethernet1/0/2 using HTTP during workday period must be mirrored to the port Ethernet1/0/20. Then, the Data Detect Server analyzes the packets.

Network Diagram

Figure 12 Network diagram for configuration of traffic mirroring



Configuration Procedure

Configure a workday period.

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] time-range a001 8:30 to 18:00 working-day
```

Define ACL 3030: Classify the packets accessing the Internet through HTTP during workday period.

```
[3Com] acl number 3030
[3Com-acl-adv-3030] rule 0 permit tcp destination 10.0.0.1 0 destina
tion-port eq 80 time-range a001
[3Com-acl-adv-3030] quit
```

Configure the port Ethernet1/0/20 as the mirroring destination port.

```
[3Com] interface Ethernet 1/0/20
[3Com-Ethernet1/0/20] monitor-port
[3Com-Ethernet1/0/20] quit
```

Configure traffic mirroring on the ports Ethernet1/0/1 and Ethernet1/0/2: Perform traffic identification through ACL 3030, and mirror the matching packets to the destination port Ethernet1/0/20.

```
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/1] mirrored-to inbound ip-group 3030 rule 0 monito
r-interface
[3Com-Ethernet1/0/1] quit
[3Com] interface Ethernet 1/0/2
[3Com-Ethernet1/0/2] mirrored-to inbound ip-group 3030 rule 0 monito
r-interface
```

*The **mirrored-to** command works only with the **permit** rules in ACLs.*

Precautions

Note the following points during the configurations:

1. When ACL rules are applied to a port, the match order of multiple rules in an ACL depends on the hardware of the switch. For the Switch 5500 Family, the match order is "first applied, last matched". Even if you configure a match order while defining an ACL, the configured one will not work.
2. Each port supports eight outbound queues. The priority of Queues 7 to 0 goes down one by one. When the SP+WRR queue scheduling algorithm is applied on a port, the switch will first schedule the queue with the weight of 0. If no packets are sent from the queue, the switch will perform the WRR scheduling for the remaining queues. When the SP+WFQ queue scheduling algorithm is applied on a port, the switch will first schedule the queue with the bandwidth of 0. If no packets are sent from the queue, the switch will perform the WFQ scheduling for the remaining queues.
3. The switch can be configured with multiple mirroring source ports but only one mirroring destination port. You are recommended to use the mirror destination port only for forwarding mirroring traffic rather than as a service port. Otherwise, normal services may be affected.
4. The **traffic-limit**, **traffic-priority**, **traffic-redirect**, and **mirrored-to** commands can work only on the **permit** rules in ACLs.
5. For the TCP/UDP port in an advanced ACL, only the **eq** operator is supported.
6. For a Layer 2 ACL, the *format-type* (including 802.3/802.2, 802.3, ether_ii, and snap) parameter is not supported.
7. All redirected packets will be tagged no matter whether the egress port is tagged.
8. When configuring a user-defined ACL, consider the following points for the offset length:
   - All the packets that are processed by the switch internally have a VLAN tag. One VLAN tag is four bytes in length.
   - If the VLAN VPN function is disabled, all the packets that are processed by the switch internally have one VLAN tag.

- If the VLAN VPN function is enabled on a port, the switch will add another layer of VLAN tag to the packets received on all ports. No matter whether the packets contain a VLAN tag originally, the packets will have two layers of VLAN tags.

The table below lists the common protocol types and offset.

Table 9 Common protocol type and offset

Protocol type	Protocol number	Offset (VLAN VPN disabled)	Offset (VLAN VPN enabled)
ARP	0x0806	16	20
RARP	0x8035	16	20
IP	0x0800	16	20
IPX	0x8137	16	20
AppleTalk	0x809B	16	20
ICMP	0x01	27	31
IGMP	0x02	27	31
TCP	0x06	27	31
UDP	0x17	27	31

Other Functions Referencing ACL Rules

Other functions that reference ACL rules are as follows:

- Telnet/SNMP/WEB login user control. For Telnet users, ACLs 2000 to 4999 may be referenced, and for SNMP/WEB users, ACLs 2000 to 2999 may be referenced.
- ACLs 2000 to 3999 can be referenced for routing policy match.
- ACLs 2000 to 3999 can be referenced for filtering route information.
- ACLs 2000 to 3999 can be referenced for displaying the routing entries that match an ACL rule.
- ACLs 2000 to 3999 can be referenced for displaying the FIB entries that match an ACL rule.
- ACLs 2000 to 3999 can be referenced for connecting a TFTP client to the TFTP server.

The functions that reference system ACL rules include:

- 802.1x function (after 802.1x is enabled globally and on a port, ACL rules are referenced to apply)
- Cluster function (the function is enabled by default. ACL rules are referenced to apply to all ports). ACL 3998 and ACL 3999 are reserved for cluster management, and cannot be configured.
- DHCP snooping (after the function is enabled, ACL rules are referenced to apply to all ports)
- Port isolation (If the function is configured and a virtual interface is available, ACL rules are referenced to apply)
- MAC+IP port binding (after the function is configured on a port, ACL rules are referenced to apply)

- Flexible QinQ (after this function is configured on a port, the ACL rules within the configured range are referenced to apply)
- Voice VLAN (if Voice VLAN is enabled on a port and an OUIMAC is available, ACL rules are referenced to add)

Configuration Example of WEB Cache Redirection

Now, only the Switch 5500 Family supports the WEB Cache redirection function.

Configuration Example of WEB Cache Redirection

Network Requirements

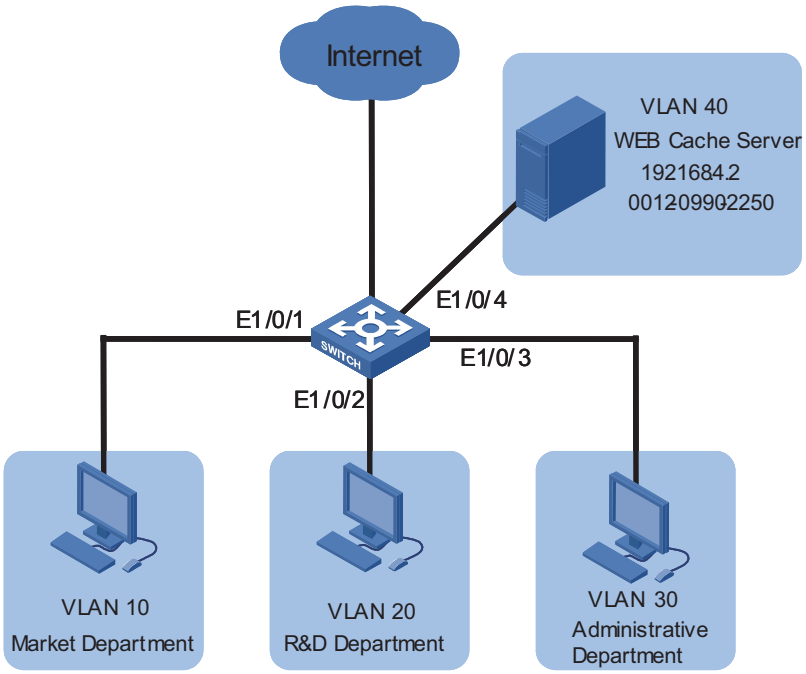
Figure 13 shows the network topology of a company. The environment is as follows:

- A Switch 5500 serves as the central switch of the company. The software version is Release 3.2.
- The marketing department gains access to the switch through the port Ethernet1/0/1. It belongs to VLAN 10, and the network segment is 192.168.1.1/24.
- The R&D department gains access to the switch through the port Ethernet1/0/2. It belongs to VLAN 20, and the network segment is 192.168.2.1/24.
- The administrative department gains access to the switch through the port Ethernet1/0/3. It belongs to VLAN 30, and the network segment is 192.168.3.1/24.
- The WEB Cache Server gains access to the switch through the port Ethernet1/0/4. It belongs to VLAN 40, and the network segment is 192.168.4.1/24.The IP address of the WEB Cache Server is 192.168.4.2, and the MAC address of it is 0012-0990-2250.

The WEB Cache redirection function is enabled on the switch, and all the packets of the marketing 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.

Network Diagram

Figure 13 Network diagram for configuration of WEB Cache redirection



Configuration Procedure

Create VLAN 10 for the marketing department, and assign an IP address 192.168.1.1 to the VLAN interface 10.

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] vlan 10
[3Com-vlan10] port Ethernet 1/0/1
[3Com-vlan10] quit
[3Com] interface Vlan-interface 10
[3Com-Vlan-interface10] ip address 192.168.1.1 24
[3Com-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.

```
[3Com] vlan 20
[3Com-vlan20] port Ethernet 1/0/2
[3Com-vlan20] quit
[3Com] interface Vlan-interface 20
[3Com-Vlan-interface20] ip address 192.168.2.1 24
[3Com-Vlan-interface20] quit
```

Create VLAN 30 for the administrative department, and assign an IP address 192.168.3.1 to the VLAN interface 30.

```
[3Com] vlan 30
[3Com-vlan30] port Ethernet 1/0/3
[3Com-vlan30] quit
[3Com] interface Vlan-interface 30
[3Com-Vlan-interface30] ip address 192.168.3.1 24
[3Com-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.

```
[3Com] vlan 40
[3Com-vlan40] port Ethernet 1/0/4
[3Com-vlan30] quit
[3Com] interface Vlan-interface 40
[3Com-Vlan-interface40] ip address 192.168.4.1 24
[3Com-Vlan-interface40] 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.

```
[3Com] webcache address 192.168.4.2 mac 0012-0990-2250 vlan 40 port
Ethernet 1/0/4
[3Com] webcache redirect-vlan 10
[3Com] webcache redirect-vlan 20
[3Com] webcache redirect-vlan 30
```

The VLAN interface 40, VLAN interface 10, VLAN interface 20, and VLAN interface 30 must be in UP state. Otherwise, the WEB Cache redirection function will not work.

3 802.1X CONFIGURATION EXAMPLE

Keywords:

802.1x and AAA

Abstract:

This article introduces the application of 802.1x on Ethernet switches in real network environments, and then presents detailed configurations of the 802.1x client, LAN Switch and AAA server respectively.

Acronyms:

AAA (Authentication, Authorization and Accounting)

The use of this document is restricted to 3Com Switch 4500, Switch 5500, Switch 5500G, Switch 4210, and Switch 4200 Families.

Introduction to 802.1X

The LAN defined in IEEE 802 protocols does not provide access authentication. In general, users can access network devices or resources in a LAN as long as they access the LAN. When it comes to application circumstances like telecom network access, building, LAN and mobile office, however, administrators need to control and configure the access of user devices. Therefore, port- or user-based access control comes into being.

802.1x is a port-based network access control protocol. It is widely accepted by vendors, service providers and end users for its low cost, superior service continuity and scalability, and high security and flexibility.

Features Configuration

Global Configuration

- Enable 802.1x globally
- Set time parameters
- Set the maximum number of authentication request attempts
- Enable the quiet timer
- Enable re-authentication upon reboot

Configuration in Port View

- Enable dot1x on the port
- Enable Guest VLAN
- Set the maximum number of users supported on the port
- Set a port access control method (port-based or MAC-based)

- Set a port access control mode (force-authorized, force-unauthorized or auto)
- Enable client version checking
- Enable proxy detection

Precautions

- The configuration of dot1x takes effect only after the dot1x feature is enabled globally.
- You can configure dot1x parameters associated with Ethernet ports or devices before enabling dot1x. However, the configured dot1x parameters only take effect after dot1x is enabled.
- The configured dot1x parameters are reserved after dot1x is disabled and will take effect if dot1x is re-enabled.

802.1X Configuration Commands

To implement 802.1x, you need to configure the supplicant system (client), authenticator system (switch) and authentication/authorization server correctly.

- Supplicant system: Ensures that the PC uses a right client.
- Authenticator system: Configuring 802.1x and AAA on the authenticator system is required.
- Authentication/authorization server: Configuring the authentication/authorization server correctly is required.

The following table shows 802.1x configuration commands necessary for configuring the switch (authenticator system). For configuration information on other devices, refer to related manuals.

Table 10 802.1x configuration commands

To...	Use the command...	Remarks
Enable 802.1x globally	**dot1x**	Required Disabled by default
Enable 802.1x on one or more ports	In system view **dot1x** [**interface** *interface-list*]	Required Disabled on a port by default
	In port view **dot1x**	802.1x must be enabled both globally in system view and on the intended port in system view or port view. Otherwise, it does not function.
Set a port access control method for the specified or all ports	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	Optional **macbased** by default Port-based access control is required for Guest VLAN.
Enable a Guest VLAN on the specified or all ports	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	Required Not enabled by default. The *vlan-id* of the Guest VLAN must be created beforehand.

Enterprise Network Access Authentication Configuration Example

The configuration or information displayed may vary with devices. The following example uses the 3Com Switch 5500 (using software V03.02.04).

Network Application Analysis

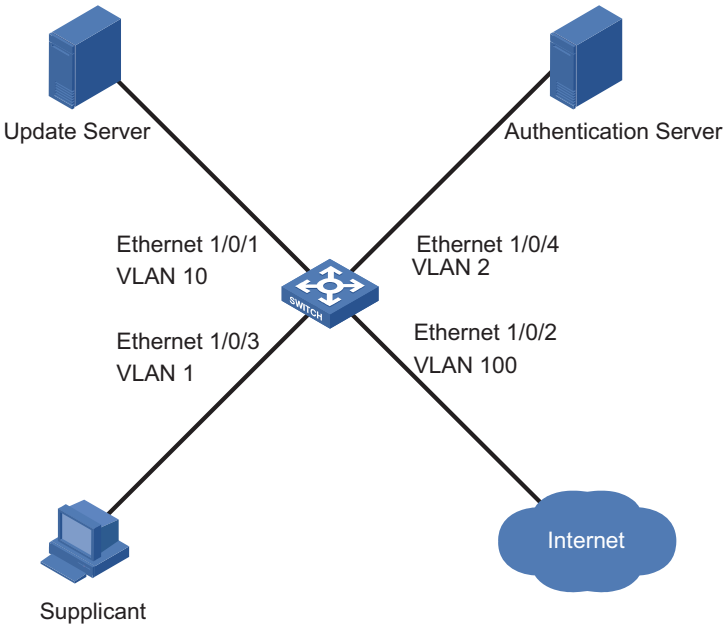
An administrator of an enterprise network needs to authenticate users accessing the network on a per-port basis on the switch to control access to network resources. Table 11 shows the details of network application analysis.

Table 11 Network application analysis

Network requirements	Solution
Access of users is controlled by authentication.	Enable 802.1x
Users can only access VLAN 10 before the authentication succeeds.	Enable Guest VLAN
Users can access VLAN 100 after the authentication succeeds.	Enable dynamic VLAN assignment
Users select the monthly payment service of 50 dollars and use 2M bandwidth to access the network.	Configure an accounting policy and bandwidth restraint policy on the RADIUS server
IP address and MAC address are bound after a user logs in.	Set MAC-to-IP binding
Tear down the connection by force if it is idle for 20 minutes.	Enable idle cut
Users can be re-authenticated successfully after the switch reboots abnormally.	Enable re-authentication upon reboot

Network Diagram

Figure 14 Network diagram for enterprise network application



Configuration Procedure

Configuring the Switch

Create a RADIUS scheme named cams, and specify the primary and secondary authentication/accounting servers.

```
<3Com> system-view
[3Com] radius scheme cams
[3Com-radius-cams] primary authentication 192.168.1.19
[3Com-radius-cams] primary accounting 192.168.1.19
[3Com-radius-cams] secondary authentication 192.168.1.20
[3Com-radius-cams] secondary accounting 192.168.1.20
```

Set the password to expert for the switch to exchange messages with the RADIUS authentication and accounting servers.

```
[3Com-radius-cams] key authentication expert
[3Com-radius-cams] key accounting expert
```

Set the username format to fully qualified user name with domain name.

```
[3Com-radius-cams] user-name-format with-domain
```

Set the server type to extended.

```
[3Com-radius-cams] server-type extended
```

Enable re-authentication upon reboot.

```
[3Com-radius-cams] accounting-on enable
```

Create an ISP domain named abc and adopt the RADIUS scheme cams for authentication.

```
[3Com] domain abc
[3Com-isp-abc] radius-scheme cams
[3Com-isp-abc] quit
```

Set the ISP domain abc as the default ISP domain.

```
[3Com] domain default enable abc
```

Enable dynamic VLAN assignment.

```
[3Com-isp-abc] vlan-assignment-mode integer
```

Enable Guest VLAN 10 on the specified port.

```
[3Com] vlan 10
[3Com-Ethernet1/0/3] dot1x port-method portbased
[3Com-Ehternet1/0/3] dot1x guest-vlan 10
```

Enable 802.1x.

```
[3Com] dot1x
```

Enable dot1x in port view.

```
[3Com-Ethernet1/0/3] dot1x
```

Use the **display** command to view the configuration associated with 802.1x and AAA parameters.

```
[3Com] display dot1x interface ethernet1/0/3
Global 802.1x protocol is enabled
 CHAP authentication is enabled
 DHCP-launch is disabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled

 Configuration: Transmit Period     30 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2

 Total maximum 802.1x user resource number is 1024
 Total current used 802.1x resource number is 0

 Ethernet1/0/3  is link-up
   802.1x protocol is enabled
   Proxy trap checker is disabled
   Proxy logoff checker is disabled
   Version-Check is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Port-based
   ReAuthenticate is disabled
   Max number of on-line users is 256

   Authentication Success: 0, Failed: 0
   EAPOL Packets: Tx 0, Rx 0
   Sent EAP Request/Identity Packets : 0
        EAP Request/Challenge Packets: 0
   Received EAPOL Start Packets : 0
            EAPOL LogOff Packets: 0
            EAP Response/Identity Packets : 0
            EAP Response/Challenge Packets: 0
            Error Packets: 0

   Controlled User(s) amount to 0

[3Com] display radius scheme cams
SchemeName  =cams                              Index=1    Type=extended
Primary Auth IP  =192.168.1.19     Port=1812
Primary Acct IP  =192.168.1.19     Port=1813
Second  Auth IP  =192.168.1.20     Port=1812
Second  Acct IP  =192.168.1.20     Port=1813
Auth Server Encryption Key= expert
Acct Server Encryption Key= expert
Accounting method = required
Accounting-On packet enable, send times = 15 , interval = 3s
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min)                             =5
Username format                                 =with-domain
Data flow unit                                  =Byte
Packet unit                                     =1
```

```
unit 1 :
Primary Auth State=active,   Second Auth State=active
Primary Acc  State=active,   Second Acc  State=active
[3Com] display domain abc
The contents of Domain abc:
   State = Active
   RADIUS Scheme = cams
   Access-limit = Disable
   Vlan-assignment-mode = Integer
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable
```

Configuring the RADIUS Server

The configuration of CAMS authentication, authorization and accounting server consists of four parts:

- "Creating an accounting policy" on page 51
- "Adding a service" on page 52
- "Adding an account user" on page 53
- "Configuring the access device" on page 54

The following parts take CAMS server V1.20 (standard version) as an example to introduce CAMS configuration.

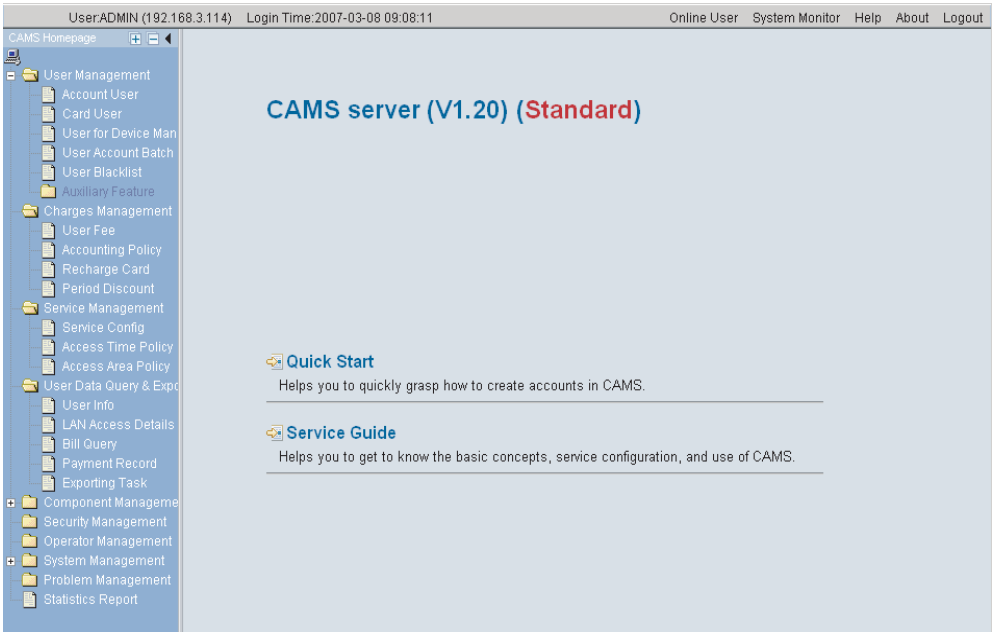
Logging in the CAMS configuration console

1 Enter the correct user name and password on the login page to log in to the CAMS configuration console.

Figure 15 Login page of CAMS configuration console

2 After login, the following page appears:

Figure 16 CAMS configuration console

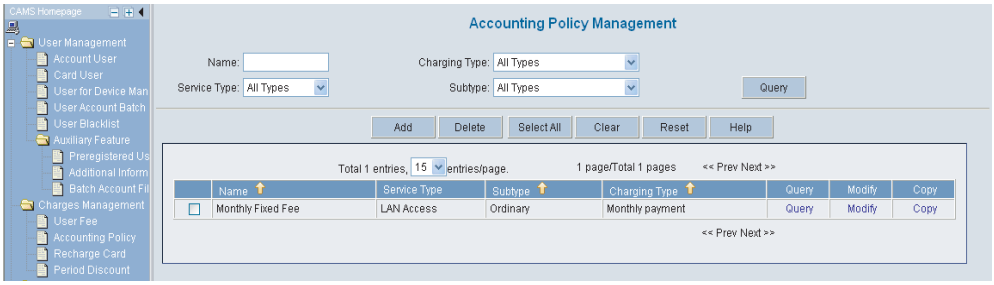


Creating an accounting policy

1 Enter the Accounting Policy Management page.

Log in the CAMS configuration console. On the navigation tree, select [Charges Management/Accounting Policy] to enter the [Accounting Policy Management] page, as shown in Figure 17.

Figure 17 Accounting Policy Management

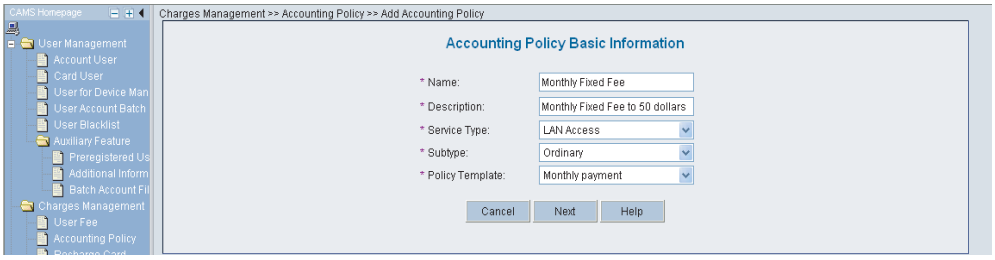


The list shows the created accounting policies. You can query, modify or maintain these policies.

2 Create an accounting policy.

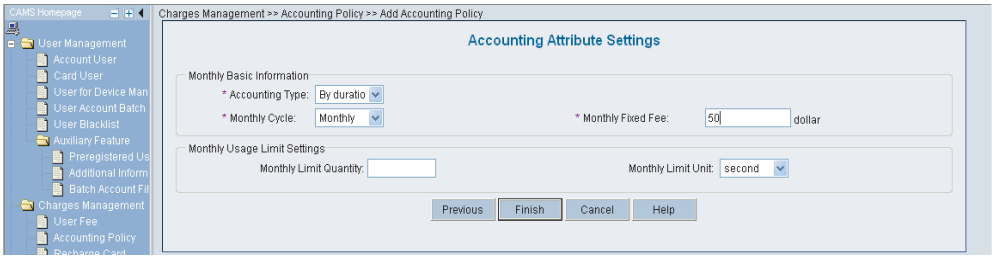
Click <Add> to enter the [Accounting Policy Basic Information] page and create a monthly payment accounting policy, as shown in Figure 18.

Figure 18 Accounting Policy Basic Information



3 Click <Next> to enter the [Accounting Attribute Settings] page, and set Accounting Type to By duration, Monthly Cycle to Monthly and Monthly Fixed Fee to 50 dollars, as shown in Figure 19.

Figure 19 Accounting Attribute Settings



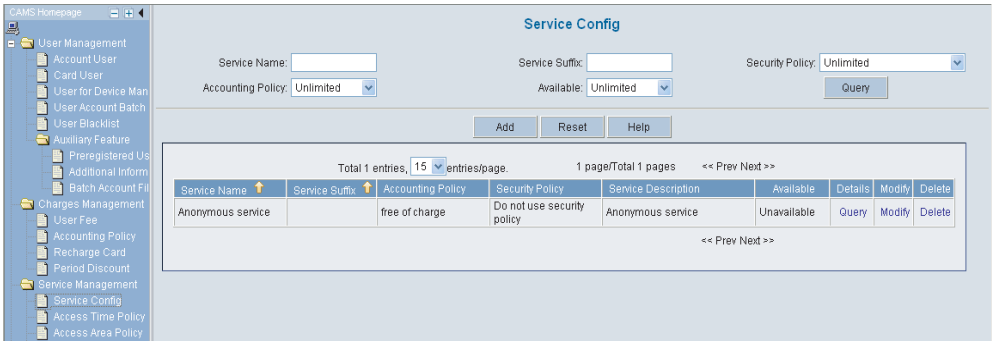
Click <OK>. A monthly payment accounting policy is created.

Adding a service

1 Enter the Service Config page.

Log in the CAMS configuration console. On the navigation tree, select [Service Management/Service Config] to enter the [Service Config] page, as shown in Figure 20.

Figure 20 Service Config



The list shows the created service types. You can query, modify or delete these service types.

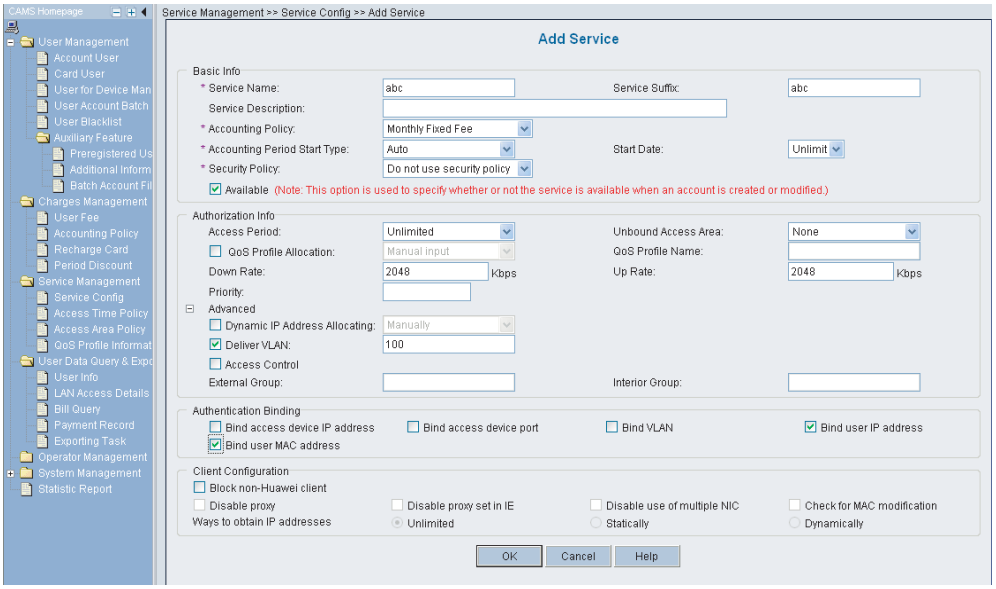
2 Add a service.

Click <Add> to enter the [Add Service] page and configure as follows:

- Service Name: abc

- Service Suffix Name: abc
- Accounting Policy: Monthly Fixed Payment
- Upstream Rate Limitation: 2M (2048 Kbps)
- Downstream Rate Limitation: 2M (2048 Kbps)
- VLAN Assignment: VLAN 100
- Authentication Binding: Bind user IP address and bind user MAC address

Figure 21 Add Service



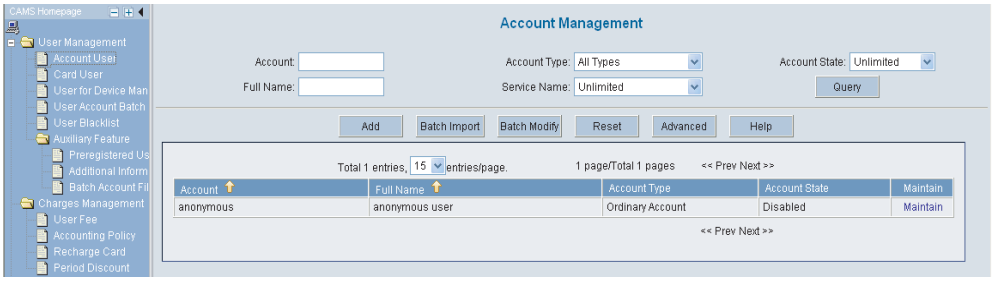
Click <OK>. A service type is added.

Adding an account user

1 Enter the Account Management page.

Log in the CAMS configuration console. On the navigation tree, select [User Management/Account User] to enter the [Account Management] page, as shown in Figure 22.

Figure 22 Account Management



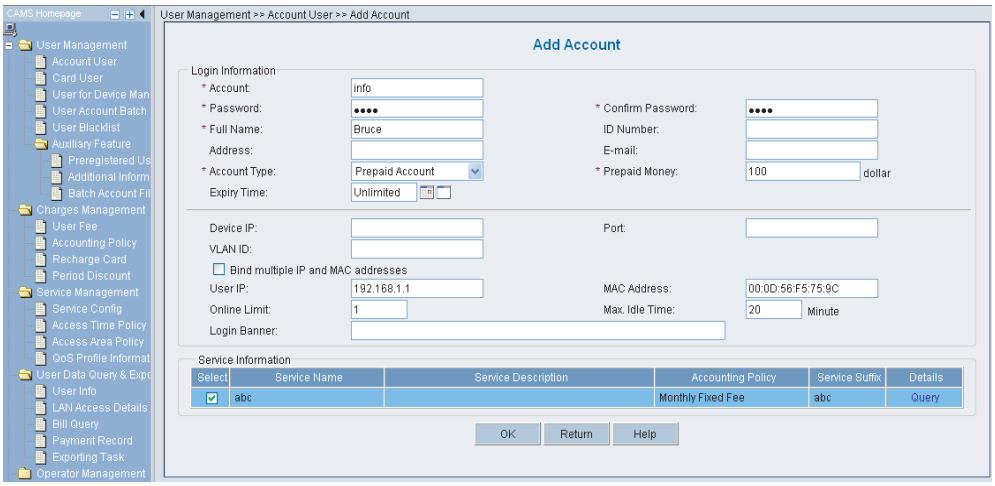
The list shows the created account users. You can maintain these account users.

2 Add an account user.

Click <Add> to enter the [Add Account] page and configure as follows:

- Account: info
- Password: info
- Full Name: Bruce
- Prepaid Money: 100 dollars
- Bind multiple IP address and MAC address: enable
- Online Limit: 1
- Max. Idle Time: 20 minutes
- Service Information: abc

Figure 23 Add Account



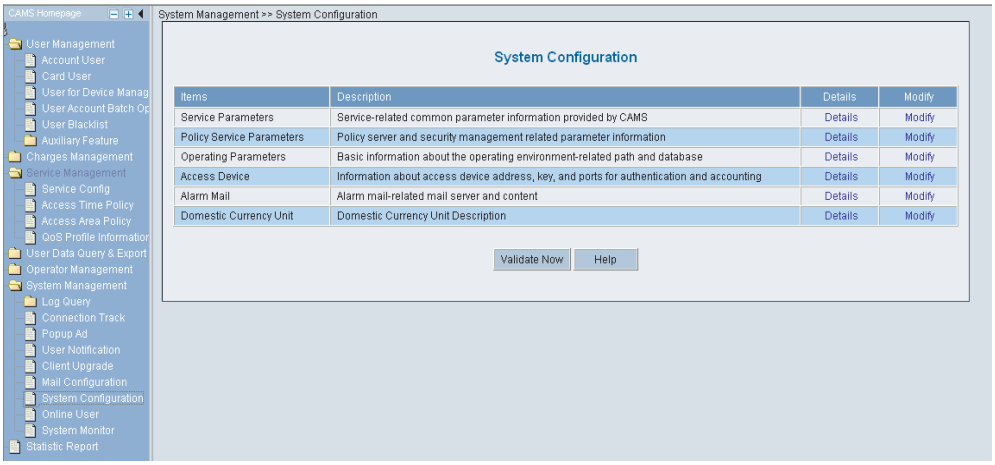
Click <OK>. An account user is added.

Configuring the access device

1 Enter the System Configuration page.

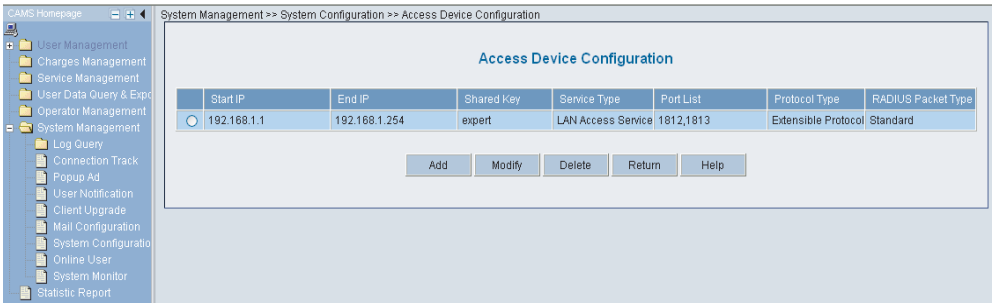
Log in the CAMS configuration console. On the navigation tree, select [System Management/System Configuration] to enter the [System Configuration] page, as shown in Figure 24.

Figure 24 System Configuration



2 Click the Modify link for the Access Device item to enter the [Access Device Configuration] page to modify access device configuration like IP address, shared key, and authentication and accounting ports.

Figure 25 Access Device Configuration



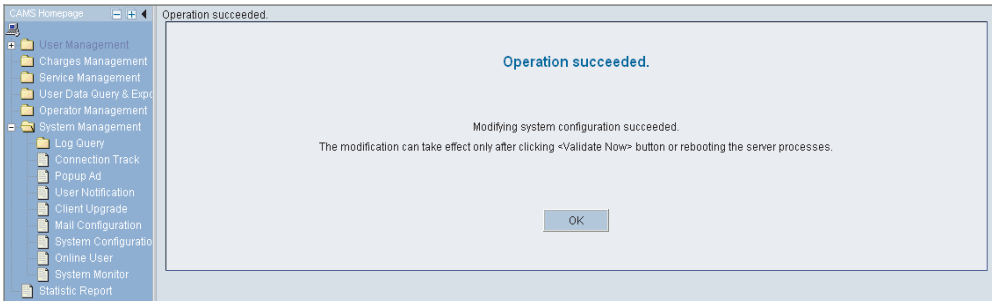
Adding configuration item

1 Click <Add> to enter the [Add Access Device] page and add configuration items, as shown in Figure 26.

Figure 26 Add Access Device

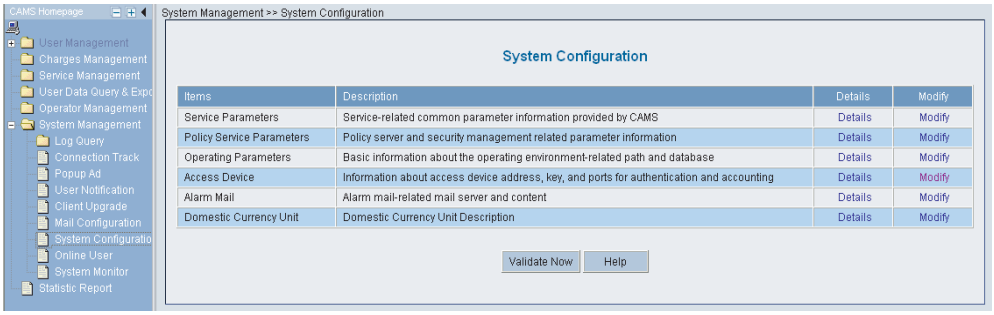
2 Click <OK>. The prompt page appears as shown in Figure 27.

Figure 27 Page prompting that system configuration is modified successfully



3 Return to the [System Configuration] page and click <Validate Now> to make the configuration take effect immediately.

Figure 28 Validate Now on System Management page

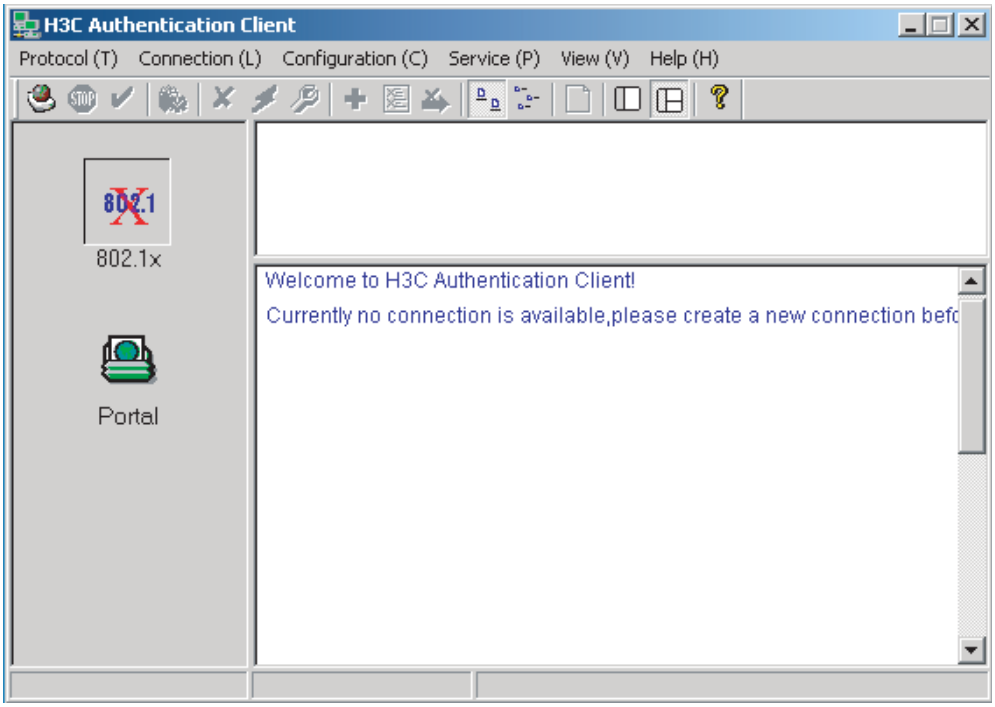


Configuring the Supplicant System

You need to install an 802.1x client on the PC, which may be 3Com's 802.1x client, the client shipped with Windows XP or other client from the third party. The following takes 3Com's 802.1X as an example to introduce how to configure the supplicant system.

Starting up 3Com authentication client

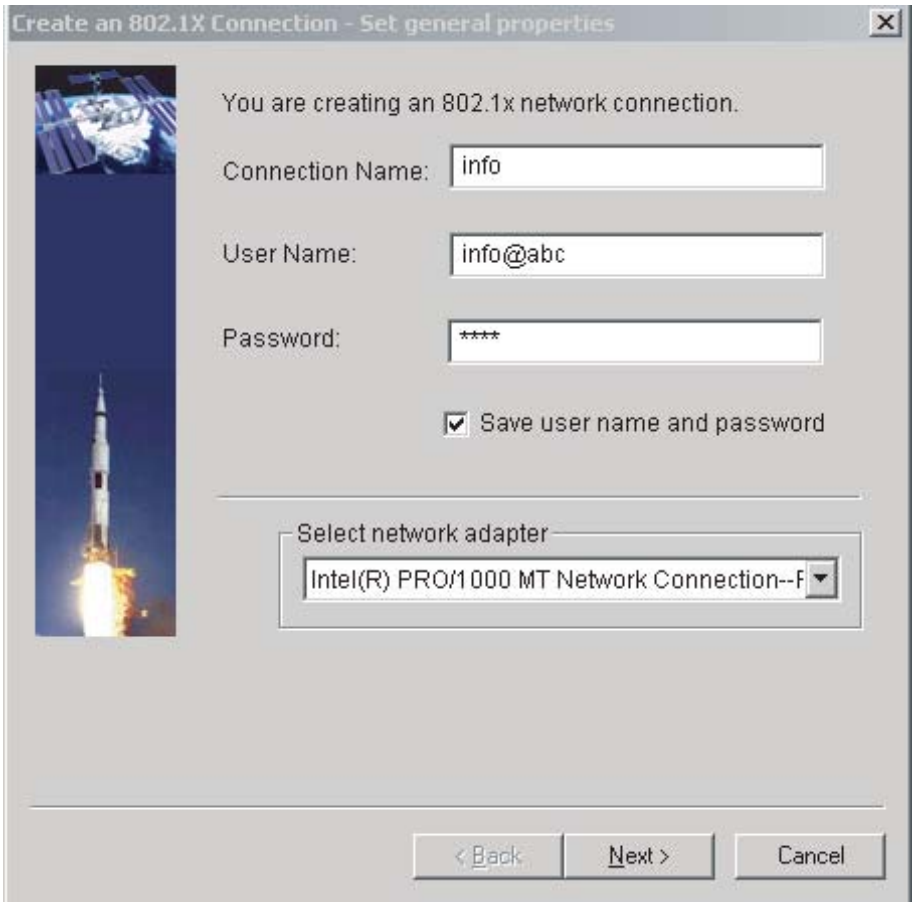
Figure 29 3Com authentication client



Creating a connection

Right click the 802.1x Authentication icon and select [Create an 802.1x connection], as shown in Figure 30.

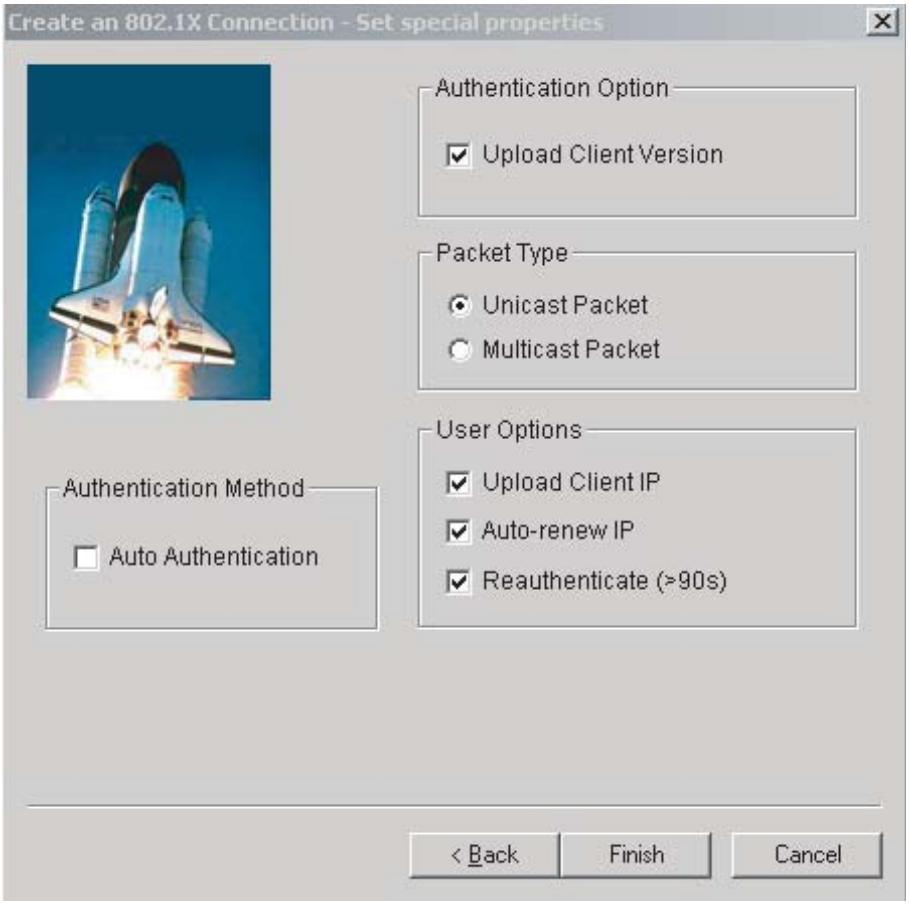
Figure 30 Create an 802.1x connection



Configuring connection attributes

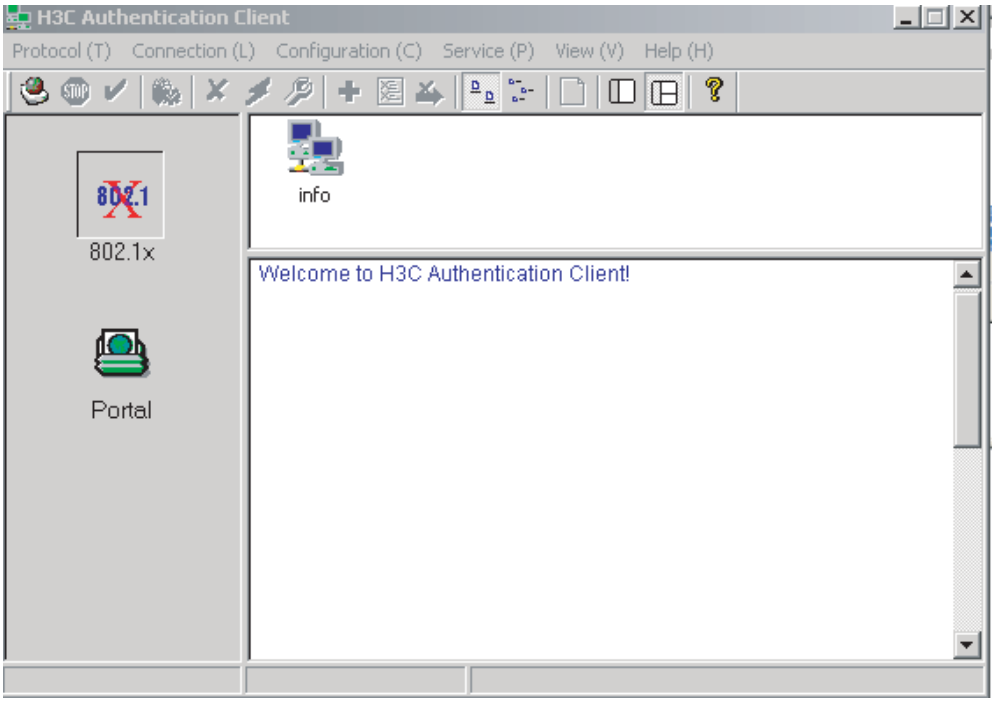
Click <Next> to enter the [Set special properties] page:

Figure 31 Set special properties



Keep default settings and click <OK>. The prompt page appears as shown in Figure 32.

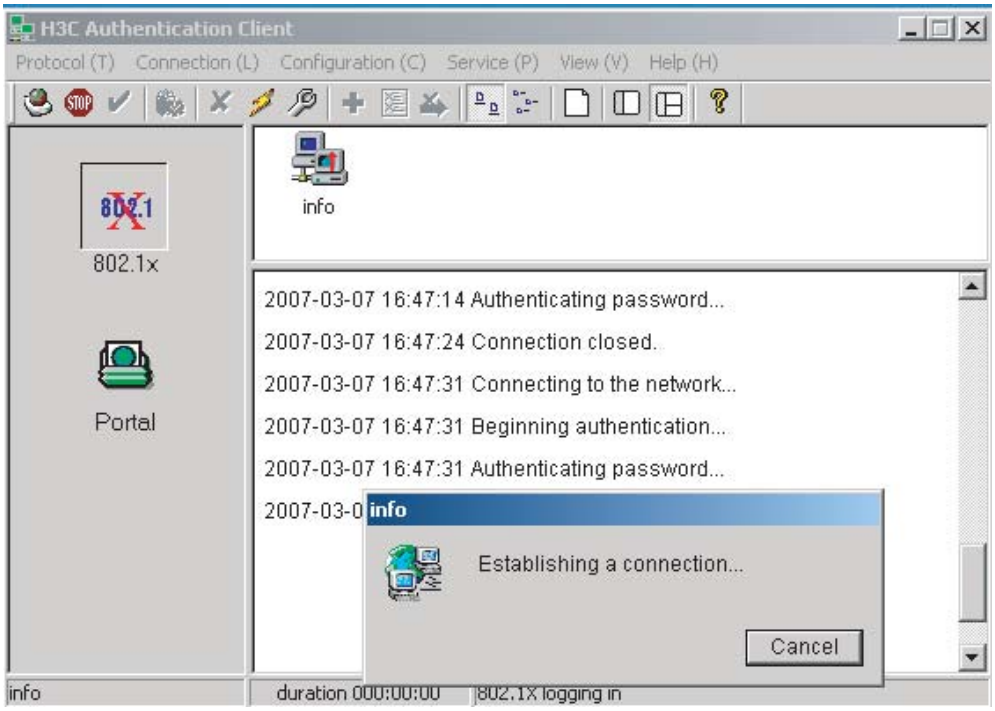
Figure 32 Page prompting that a connection is created successfully



Initiating the connection

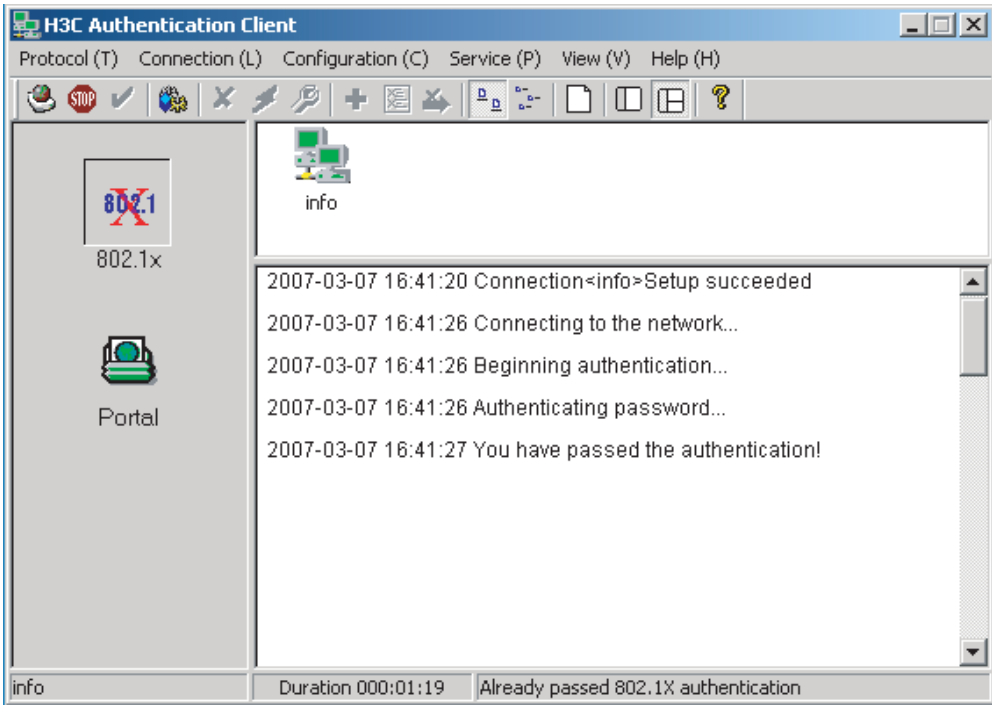
Double click the info connection:

Figure 33 Connecting



The connection succeeds:

Figure 34 Page prompting that the Authentication succeeds



Verifying Configuration

To verify that the configuration of Guest VLAN is taking effect, check that users can access VLAN 10 before 802.1x authentication or the 802.1x authentication fails.

To verify that the dynamically assigned VLAN is taking effect, check that users can access VLAN 100 after 802.1x authentication succeeds. At the same time, 802.1x authentication cooperates with CAMS to complete accounting and real time monitoring.

To verify that the configuration of IP-to-MAC binding is taking effect, check that users can be re-authenticated and access the Internet when the device reboots abnormally. If the configured IP-to-MAC binding is different from that on the CAMS, the user cannot access the Internet.

Troubleshooting

Symptom: 802.1x authentication failed

Solution:

- Use the **display dot1x** command to verify 802.1x is enabled globally and on the specified ports.
- Verify the username and password are set correctly.
- Verify the connection works well.
- Use the **debugging dot1x packet** command to verify the switch receives and sends EAP and EAPoL packets normally.

Symptom: Users can access network resources without 802.1x authentication

- Use the **display dot1x** command to verify 802.1x is enabled globally and on the specified ports.

- Use the **display interface** command to verify the statistics of incoming packets are available for the specified port. 802.1x authentication applies only to incoming packets, not outgoing packets.

4 SSH CONFIGURATION EXAMPLE

Keywords:

SSH, RSA

Abstract:

This article introduces the application of SSH on the 3Com stackable switches in real network environments, and then presents detailed configurations of the involved SSH client and Ethernet switches respectively.

Acronyms:

SSH (Secure Shell), RSA (Rivest Shamir Adleman)

Introduction to SSH

Secure Shell (SSH) is designed to provide secure remote login and other security services in insecure network environments. When users remotely access the switch across an insecure network, SSH will automatically encrypt data before transmission and decrypt data after they reach the destination to guarantee information security and protect switches from such attacks as plain-text password interception. In addition, SSH provides powerful authentication to defend against the man-in-the-middle attacks. SSH uses the client/server mode, by which the SSH server accepts the connection requests from SSH clients and provides authentication. SSH clients can establish SSH connections and log into the SSH server through the SSH connections.

SSH also provides other functions, such as compressing the data to be transmitted to speed up the transmission speed, functioning as Telnet, and providing secure channels for FTP, PoP and even PPP.

For details about SSH functions supported on different Ethernet switches, refer to related user manuals.

Support for SSH Functions

Table 12 List of SSH functions supported on the 3Com stackable switches

Model\Function	SSH server	SSH client
Switch 5500	●	●
Switch 4500	●	●
Switch 5500G	●	●
Switch 4200	●	●
Switch 4200G	●	●
Switch 4210	●	●

SSH Configuration

Configuring an SSH Server

For a 3Com switch to be the SSH server

- Configure the protocols supported on user interfaces
- Create or destroy a RSA key pair
- Export a RSA key pair
- Create an SSH user and specify an authentication type
- Specify a service type for the SSH user
- Configure the SSH management function on the SSH server
- Configure a client public key on the SSH server
- Specify a public key for the SSH user
- Specify the source IP address or source interface of packets

For a non 3Com device to be the SSH server

For such configuration, refer to the related user manual.

Configuring an SSH Client

Using SSH client software

There are many kinds of SSH client software, such as PuTTY, Tectia, Winscp, and OpenSSH. You can select one as required and refer to the attached manual for configuration.

Using an SSH2-capable switch

- Configure whether first-time authentication is supported
- Establish a connection between the SSH client and the SSH server

Precautions

- If you have configured a user interface to support the SSH protocol, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command to ensure successful login.
- Creating a RSA key pair on the SSH server is necessary for successful SSH login.
- For new SSH users to login successfully, you must specify an authentication type for them.

SSH Configuration Commands

To implement SSH, you need to configure the SSH client and the SSH server correctly.

The following sections describe switch's SSH configuration commands. For more information, refer to the SSH section of the applicable configuration guide.

Configuring an 3Com Switch as an SSH Server

Configuration Procedure

Table 13 Configure the switch as an SSH server

Role	Common configuration	Authentication type	Public key configuration		Remarks
SSH server	For detailed command, refer to "Common configuration" on page 66.	Password authentication	-		For detailed command, refer to "Password authentication configuration" on page 67.
		RSA authentication	Configure a public key manually: copy the public key from the client public key file to the SSH server.	Associate the client public key saved on the SSH server to the SSH client	For detailed commands, refer to "Configuring the client RSA public key manually" on page 67.
			Import a public key: import the public key from the client public file to the SSH server through commands.		For detailed commands, refer to "Importing the client RSA public key" on page 68 .

Precautions for authentication type configuration

The above table introduces the password authentication and RSA authentication separately. In practice, you can combine the two authentication types.

- Executing the **ssh authentication-type default password-publickey** command or the **ssh user authentication-type password-publickey** command means that users must not only pass the password authentication but also pass the RSA authentication to login the SSH server.
- Executing the **ssh authentication-type default all** command or the **ssh user authentication-type all** command means that users can login the SSH server as long as they pass either the password or RSA authentication.

Public key configuration procedure and precautions

As shown in Table 13, you need to copy or import the public key from the client to the server.

1 Manually configure the RSA public key

- When a switch acts as the SSH client, use the **display rsa local-key-pair public** command to display the RSA public key after creating RSA key pair through the corresponding commands.
- Manually copy the RSA public key to the SSH server. Thus, the SSH server has the same public key as the SSH client, and can authenticate the SSH client when the SSH client establishes a connection with it.

2 Import the RSA public key

- When a switch acts as the SSH server, use the SSH client software to generate an RSA key pair, and then upload the RSA public key file to the SSH server through FTP or TFTP.
- On the SSH server, import the public key from the public key file through commands.

3 Precautions

When some SSH client software like PuTTY is used to generate an RSA key pair, you can either manually configure the public key for the SSH server or import the public key to the SSH server.

Configuration Commands

Common configuration

Table 14 Common configuration

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter the view of one or multiple user interfaces	**user-interface** [*type-keyword*] *number* [*ending-number*]	-
Configure the authentication mode as scheme	**authentication-mode scheme** [**command-authorization**]	Required By default, the user interface authentication mode is password.
Specify the supported protocol(s)	**protocol inbound** { **all** |**ssh** | **telnet** }	Optional By default, both Telnet and SSH are supported.
Return to the system view	**quit**	-
Create an RSA key pair	**rsa local-key-pair create**	Required By default, no RSA key pair is created.
Destroy the RSA key pair	**rsa local-key-pair destroy**	Optional
Specify a service type for the SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	Optional **stelnet** by default
Set SSH authentication timeout time	**ssh server timeout** *seconds*	Optional By default, the timeout time is 60 seconds.
Set SSH authentication retry times	**ssh server authentication-retries** *times*	Optional By default, the number of retry times is 3.
Set RSA server key update interval	**ssh server rekey-interval** *hours*	Optional By default, the system does not update RSA server keys.
Configure SSH server to be compatible with SSH1.x clients	**ssh server compatible-ssh1x enable**	Optional By default, SSH server is compatible with SSH1.x clients.

Table 14 Common configuration

Operation	Command	Remarks
Specify a source IP address for the SSH server	**ssh-server source-ip** *ip-address*	Optional
Specify a source interface for the SSH server	**ssh-server source-interface** *interface-type interface-number*	Optional

Password authentication configuration

Table 15 Configure password authentication

Operation	Command		Description
Create an SSH User and specify an authentication type	Specify the default authentication type for all SSH users	**ssh authentication-type default password**	Use either command. By default, no SSH user is created and no authentication type is specified. Note that: If both commands are used and different authentication types are specified, the authentication type specified with the **ssh user authentication-type** command takes precedence.
		ssh user *username*	
	Create an SSH user, and specify an authentication type for the user	**ssh user** *username* **authentication-type password**	

For common configuration commands, refer to Table 14.

Configuring the client RSA public key manually

Table 16 Configure the client RSA public key manually

Operation	Command		Description
Create an SSH user and specify an authentication type	Specify the default authentication type for all SSH users	**ssh authentication-type default rsa**	Use either command. By default, no SSH user is created and no authentication type is specified. Note that: If both commands are used and different authentication types are specified, the authentication type specified with the **ssh user authentication-type** command takes precedence.
		ssh user *username*	
	Create an SSH user, and specify an authentication type for it	**ssh user** *username* **authentication-typ rsa**	
Enter public key view	**rsa peer-public-key** *keyname*		Required
Enter public key edit view	**public-key-code begin**		-
Configure the client RSA public key	Enter the content of the RSA public key		The content must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCS. Spaces and carriage returns are allowed between characters.

Table 16 Configure the client RSA public key manually

Operation	Command	Description
Return from public key code view to public key view	**public-key-code end**	When you exit public key code view, the system automatically saves the public key.
Return from public key view to system view	**peer-public-key end**	-
Assign a public key to an SSH user	**ssh user** *username* **assign rsa-key** *keyname*	Required If you issue this command multiple times, the last command overrides the previous ones

For general configuration commands, refer to Table 14.

Importing the client RSA public key

Table 17 Import the client RSA public key

Operation	Command		Description
Create an SSH user and specify an authentication type	Specify the default authentication type for all SSH users	**ssh authentication-type default rsa**	Use either command. By default, no SSH user is created and no authentication type is specified. Note that: If both commands are used and different authentication types are specified, the authentication type specified with the **ssh user authentication-type** command takes precedence.
		ssh user *username*	
	Create an SSH user, and specify an authentication type for it	**ssh user** *username* **authentication-type rsa**	
Import the client RSA public key from the specified public key file	**rsa peer-public-key** *keyname* **import sshkey** *filename*		Required
Assign a public key to an SSH user	**ssh user** *username* **assign rsa-key** *keyname*		Required If you issue this command multiple times, the last command overrides the previous ones

For general configuration commands, refer to Table 14.

Configuring an 3Com Switch as an SSH Client

When the device connects to the SSH server as an SSH client, you can configure whether the device supports first-time authentication.

- First-time authentication means that when the SSH client accesses the server for the first time and is not configured with the server host public key, the user can continue accessing the server, and will save the host public key on the client for use in subsequent authentications.
- When first-time authentication is not supported, a client, if not configured with the server host public key, will be denied of 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.

Configuration Procedure

Table 18 Configure the switch as an SSH client

Role	Common configuration	First-time authentication support	Public key configuration		Access the SSH server	Remarks
SSH Client	Refer to "Common configuration" on page 69.	Yes	--		Establish a connection between the SSH client and the SSH server	Refer to "Enabling first-time authentication" on page 69.
		No	Configure a public key manually: copy the server public key from the public key file to the SSH client	Specify the host public key of the SSH server to be connected		Refer to "Disabling first-time authentication and manually configuring the server public key" on page 70.

As shown in Table 18, you need to configure the server public key to the client in the case that the SSH client does not support first-time authentication.

1 Manually configure the RSA public key

- On the SSH server, use the **display rsa local-key-pair public** command to display the RSA public key.
- Manually copy the public key to the SSH client. Thus, the SSH client has the same public key as the SSH server, and can authenticate the SSH server using the public key when establishing a connection with the SSH server.

Configuration Commands

Common configuration

Table 19 Common configuration

Operation	Command	Description
Enter system view	**system-view**	-
Specify a source IP address for the SSH client	**ssh2 source-ip** *ip-address*	Optional
Specify a source interface for the SSH client	**ssh2 source-interface** *interface-type interface-number*	Optional

Enabling first-time authentication

Table 20 Enable first-time authentication

Operation	Command	Description
Enter system view	**system-view**	-
Enable first-time authentication	**ssh client first-time enable**	Optional Enabled by default

Table 20 Enable first-time authentication

Operation	Command	Description
Establish a connection with the SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client.

Disabling first-time authentication and manually configuring the server public key

Table 21 Disable first-time authentication and manually configure the server public key

Operation	Command	Description
Enter system view	**system-view**	--
Disable first-time authentication	**undo ssh client first-time**	Required Enabled by default
Enter public key view	**rsa peer-public-key** *keyname*	Required
Enter public key edit view	**public-key-code begin**	-
Configure server public key	Enter the content of the public key	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 <Enter> 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.
Return to public key view from public key edit view	**public-key-code end**	When you exit public key code view, the system automatically saves the public key
Exit public key view and return to system view	**peer-public-key end**	-
Specify the host key name of the server	**ssh client** { *server-ip* | *server-name* } **assign rsa-key** *keyname*	Optional Required when the SSH client does not support first-time authentication You need to copy the server public key to the SSH client before performing this configuration.

Table 21 Disable first-time authentication and manually configure the server public key

Operation	Command	Description
Start the client to establish a connection with an SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client.

SSH Configuration Example

The Switch 5500 software version in this configuration example is Release V03.02.04.

When the Switch Acts as the SSH Server and the Authentication Type is Password

Network requirements

As shown in Figure 35, 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 35 Network diagram of SSH server configuration using password authentication

Configuration procedure

1 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate RSA key pairs.

```
[3Com] rsa local-key-pair create
```

Set the authentication mode for the user interfaces to AAA.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
[3Com-ui-vty0-4] quit
```

Create local client "client001", and set the authentication password to "abc", protocol type to SSH, and command privilege level to 3 for the client.

```
[3Com] local-user client001
[3Com-luser-client001] password simple abc
[3Com-luser-client001] service-type ssh level 3
[3Com-luser-client001] quit
```

Specify the authentication method of user client001 as password.

```
[3Com] ssh user client001 authentication-type password
```

2 Configure the SSH client

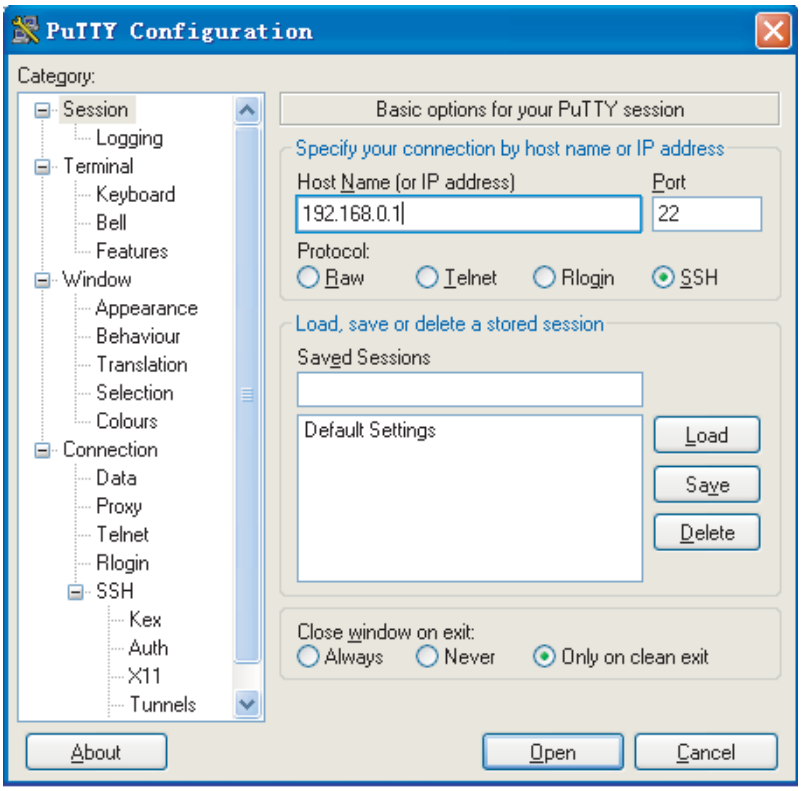
Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server.

Take SSH client software "Putty" (version 0.58) as an example:

- Run PuTTY.exe to enter the following configuration interface.

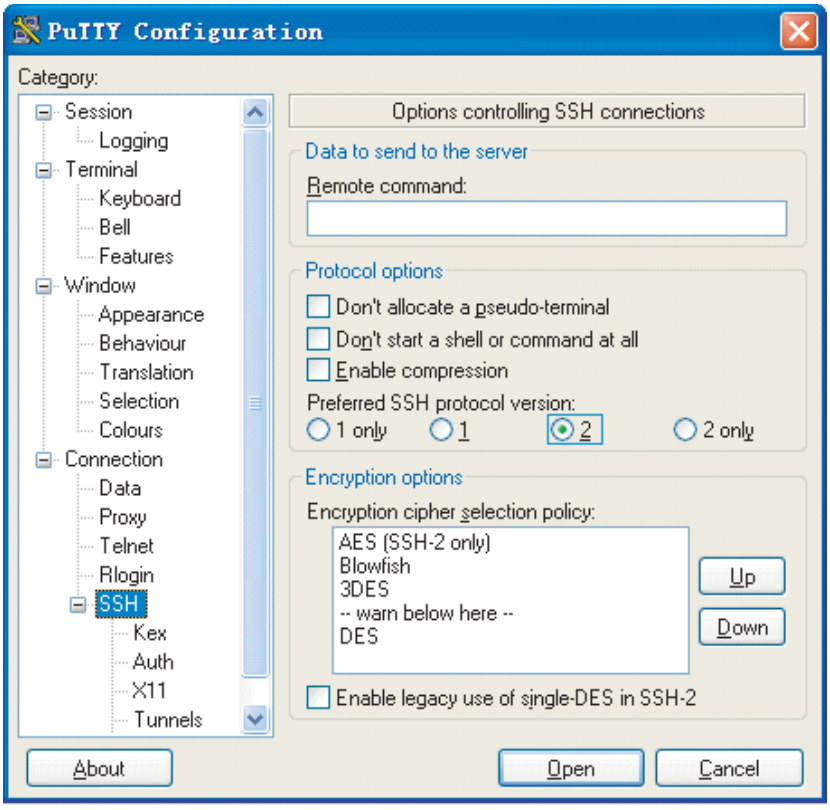
Figure 36 SSH client configuration interface



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

- From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 37 appears.

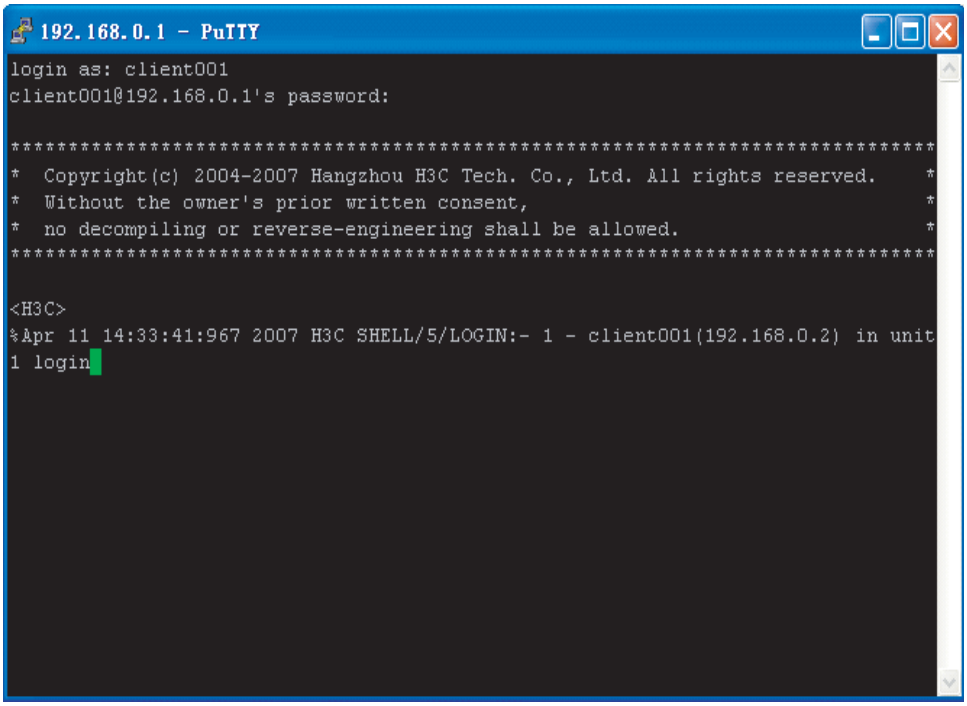
Figure 37 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

- As shown in Figure 38, click **Open** to enter the following interface. If the connection is normal, you will be prompted to enter the user name "client001" and password "abc". Once authentication succeeds, you will log onto the server.

Figure 38 SSH client interface



When the Switch Acts as an SSH Server and the Authentication Type is RSA

Network requirements

As shown in Figure 39, 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. RSA authentication is required.

Network diagram

Figure 39 Network diagram of SSH server configuration

Configuration procedure

1 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate RSA key pairs.

```
[3Com] rsa local-key-pair create
```

Set the authentication mode for the user interfaces to AAA.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
```

Set the client's command privilege level to 3

```
[3Com-ui-vty0-4] user privilege level 3
[3Com-ui-vty0-4] quit
```

Configure the authentication type of the SSH client named client 001 as RSA.

```
[3Com] ssh user client001 authentication-type rsa
```

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 an SSH Client" on page 64.

Import the client's public key named "Switch001" from file "public".

```
[3Com] rsa peer-public-key Switch001 import sshkey public
```

Assign the public key "Switch001" to client "client001".

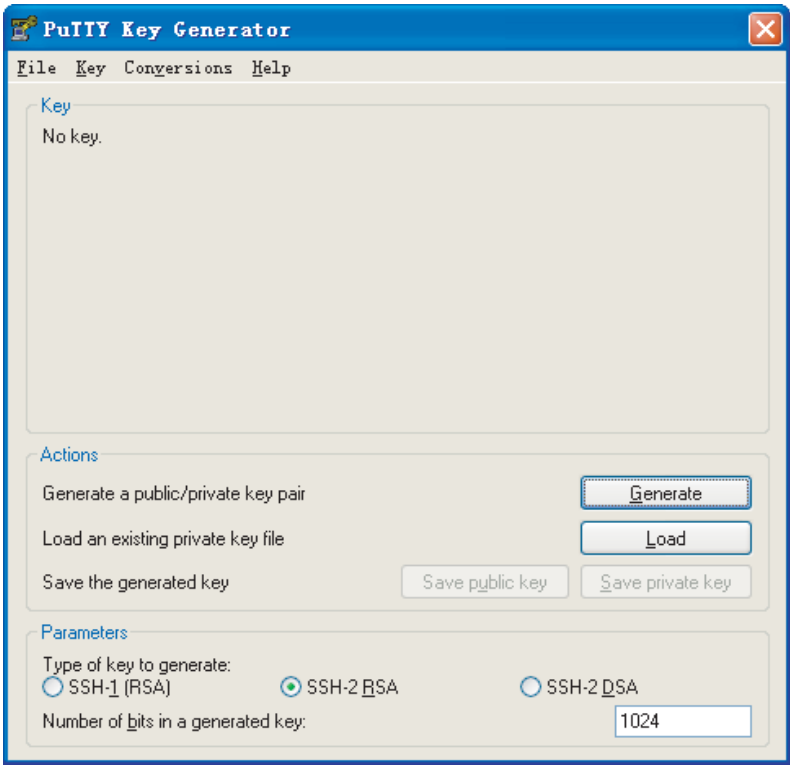
```
[3Com] ssh user client001 assign rsa-key Switch001
```

2 Configure the SSH client

Generate an RSA key pair, taking PuTTYGen as an example.

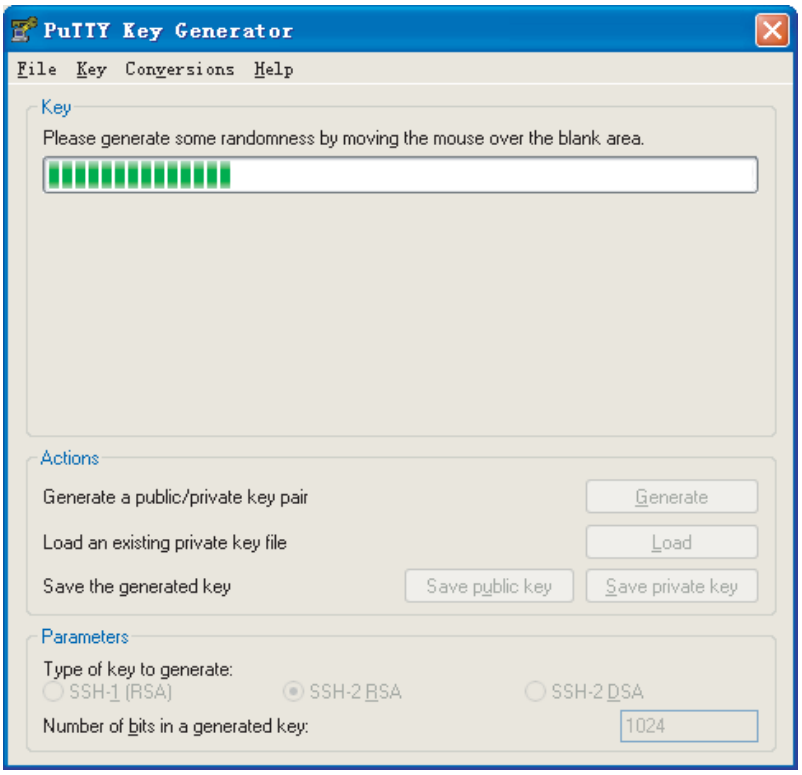
- Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

Figure 40 Generate a client key pair (1)



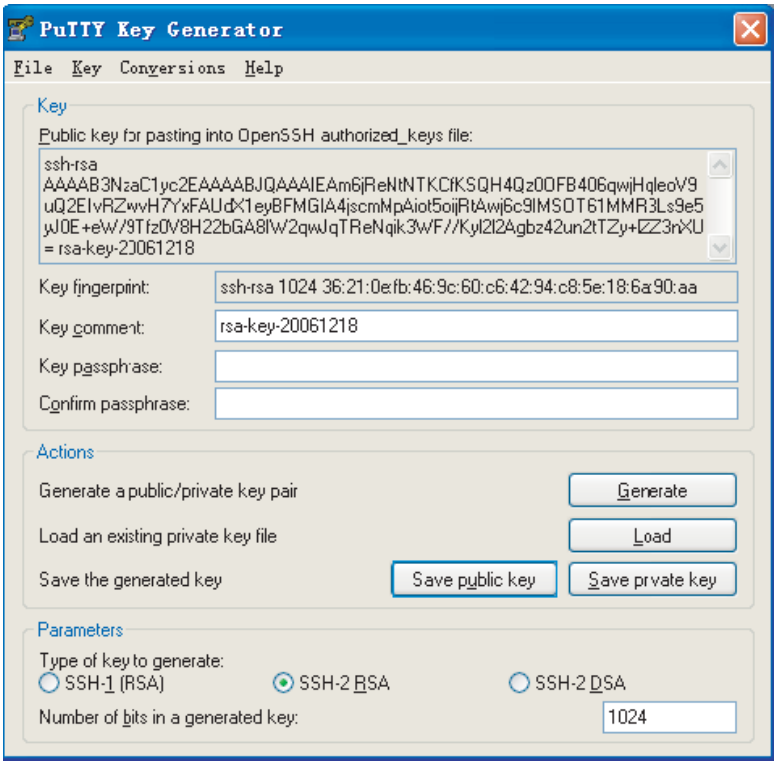
While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in Figure 40. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 41 Generate a client key pair (2)



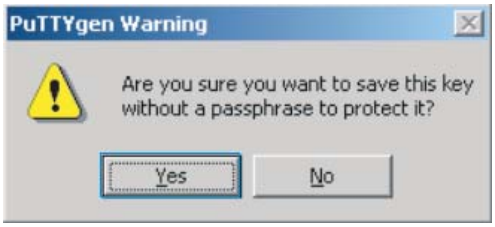
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key ("public" in this case).

Figure 42 Generate a client key pair (3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the private key ("private.ppk" in this case).

Figure 43 Generate a client key pair (4)



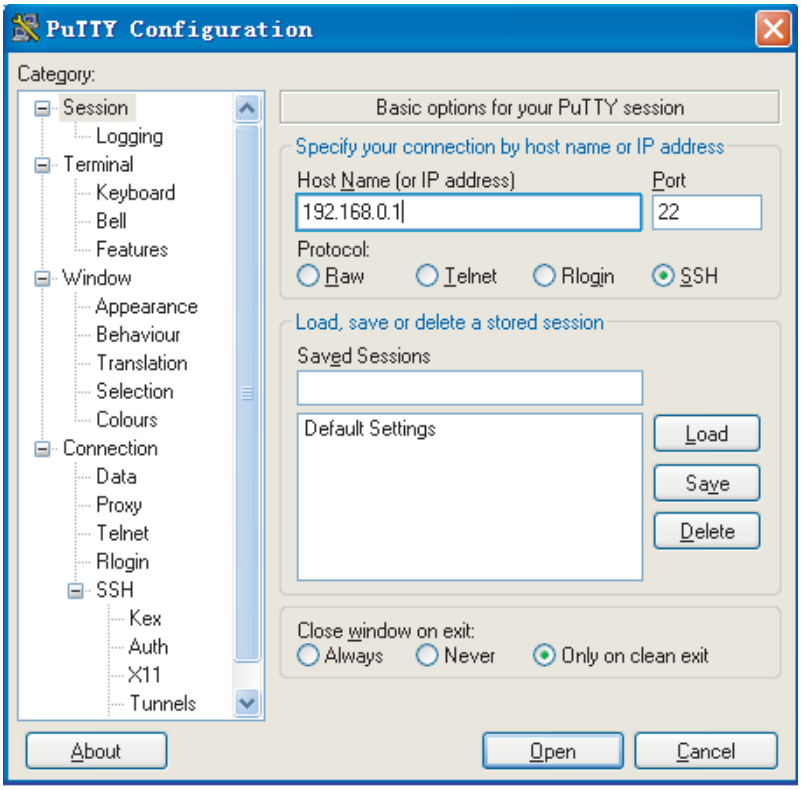
After a public key pair is generated, you need to upload the pubic key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

Establish a connection with the SSH server.

The following takes the SSH client software Putty (version 0.58) as an example.

- Launch PuTTY.exe to enter the following interface.

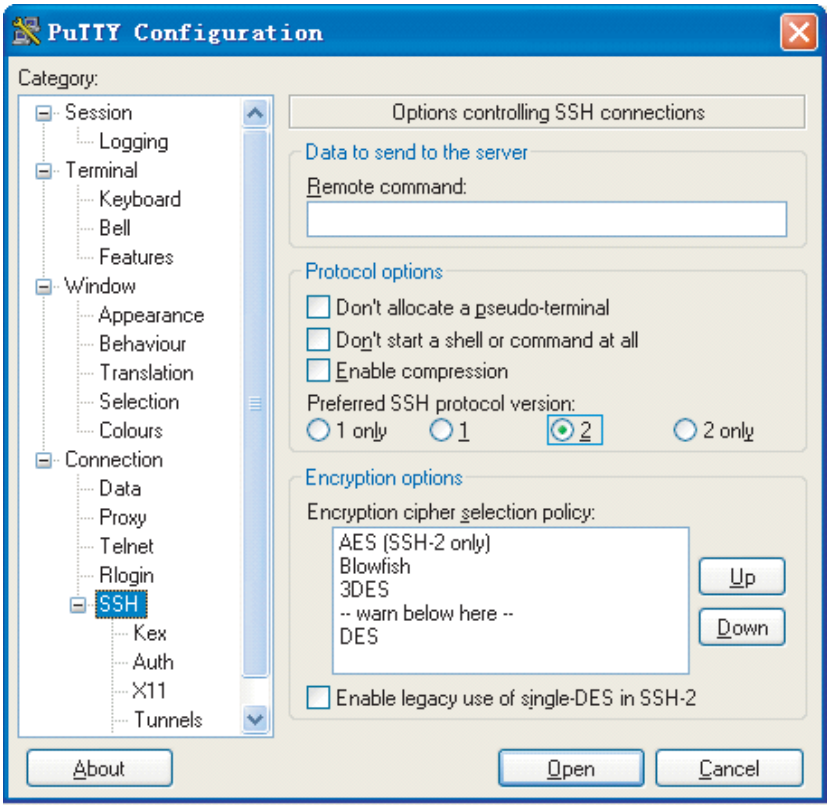
Figure 44 SSH client configuration interface 1



In the **Host Name (or IP address)** text box, enter the IP address of the server.

- From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 45 appears.

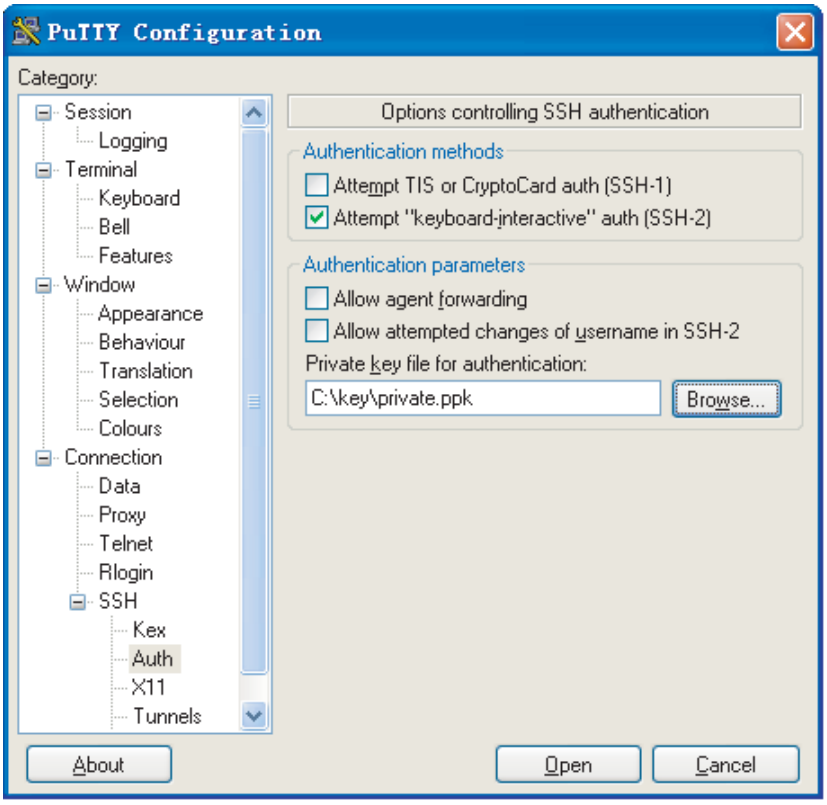
Figure 45 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

- Select **Connection/SSH/Auth**. The following window appears.

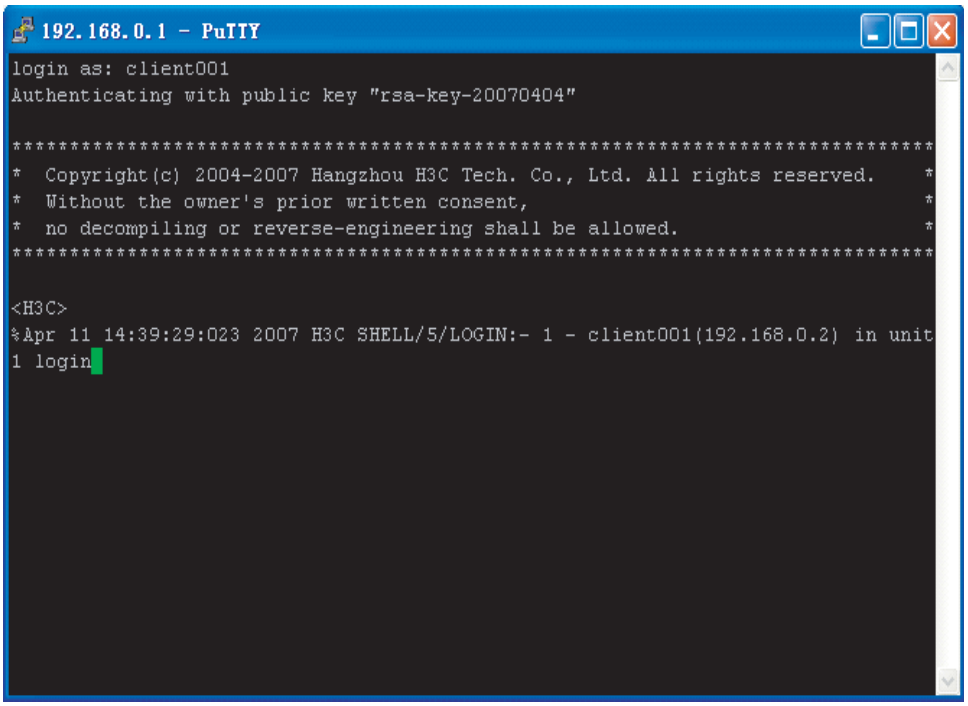
Figure 46 SSH client configuration interface (2)



Click **Browse...** to bring up the file selection window, navigate to the private key file and click **OK**.

- From the window shown in Figure 46, click **Open**. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 47.

Figure 47 SSH client interface



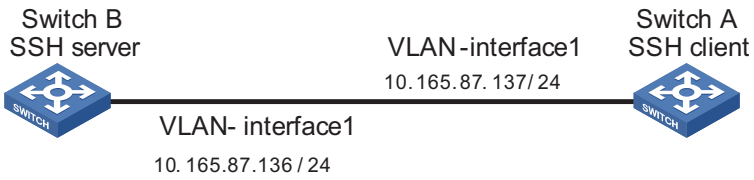
When the Switch Acts as an SSH Client and the Authentication Type is Password

Network requirements

As shown in Figure 48, 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 48 Network diagram of SSH client configuration when using password authentication



Configuration procedure

1 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate RSA key pairs.

```
[3Com] rsa local-key-pair create
```

Set the authentication mode for the user interfaces to AAA.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
[3Com-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.

```
[3Com] local-user client001
[3Com-luser-client001] password simple abc
[3Com-luser-client001] service-type ssh level 3
[3Com-luser-client001] quit
```

Configure the authentication type of user client001 as password.

```
[3Com] ssh user client001 authentication-type password
```

2 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[3Com-Vlan-interface1] quit
```

Establish a connection to the server 10.165.87.136.

```
[3Com] 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) 2004-2006 Hangzhou 3Com Technologies Co., Ltd.          *
* Without the owner's prior written consent,                           *
* no decompiling or reverse-switch fabricering shall be allowed.       *
************************************************************************

<3Com>
```

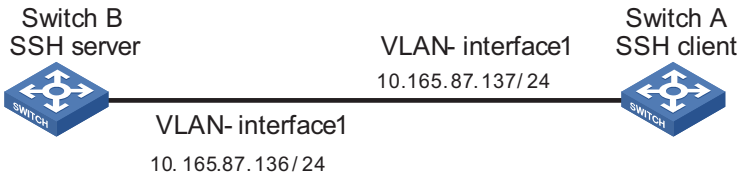
When the Switch Acts as an SSH Client and the Authentication Type is RSA

Network requirements

As shown in Figure 49, 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. RSA authentication is required.

Network diagram

Figure 49 Network diagram of SSH client configuration when using publickey authentication



Configuration procedure

1 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate RSA key pair.

```
[3Com] rsa local-key-pair create
```

Set the authentication mode for the user interfaces to AAA.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[3Com-ui-vty0-4] user privilege level 3
[3Com-ui-vty0-4] quit
```

Specify the authentication type of user client001 as RSA.

```
[3Com] ssh user client001 authentication-type rsa
```

Before proceeding with the following steps, you need to generate an RSA key pair on the client, and manually configure the RSA public key for the SSH server. For detailed information, refer to "Configuring an SSH Client" on page 64.

Configure the public key of the SSH client on the SSH server, and specify the public key name as Switch001.

```
[3Com] rsa peer-public-key Switch001
RSA public key view: return to System View with "peer-public-key end".
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[3Com-rsa-key-code] 3047
[3Com-rsa-key-code] 0240
```

```
[3Com-rsa-key-code] C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
[3Com-rsa-key-code] 349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
[3Com-rsa-key-code] 74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
[3Com-rsa-key-code] 074C0CA9
[3Com-rsa-key-code] 0203
[3Com-rsa-key-code] 010001
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[3Com]
```

Assign the public key Switch001 to user client001.

```
[3Com] ssh user client001 assign rsa-key Switch001
```

2 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate a RSA key pair

```
[3Com] rsa local-key-pair create
```

Display the RSA public key on the client.

```
<3Com> display rsa local-key-pair public

=====================================================
Time of Key pair created: 05:15:04  2006/12/08
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
    349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
    74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
    074C0CA9
  0203
    010001
<Omitted>
```

After generating an RSA key pair on the client, you need to configure the RSA public key for the SSH server and finish the SSH server configuration before continuing to configure the SSH client.

Establish an SSH connection to the server 10.165.87.136.

```
[3Com] 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

**************************************************************************
* Copyright(c) 2004-2006 Hangzhou 3Com Technologies Co., Ltd.           *
* Without the owner's prior written consent,                            *
* no decompiling or reverse-switch fabricering shall be allowed.        *
**************************************************************************

<3Com>
```

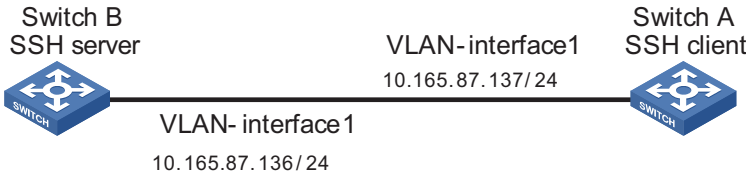
When the Switch Acts as an SSH Client and First-time authentication is not Supported

Network requirements

As shown in Figure 50, 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 **RSA** authentication mode is used to enhance security.

Network diagram

Figure 50 Network diagram of SSH client configuration



Configuration procedure

1 Configure Switch B

Create a VLAN interface on the switch and assign an IP address for it to serve as the destination of the client.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate RSA key pairs.

```
[3Com] rsa local-key-pair create
```

Set AAA authentication on user interfaces.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Configure the user interfaces to support SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[3Com-ui-vty0-4] user privilege level 3
[3Com-ui-vty0-4] quit
```

Specify the authentication type for user client001 as RSA.

```
[3Com] ssh user client001 authentication-type rsa
```

Before proceeding with the following steps, you need to generate an RSA key pair on the client, and manually configure the RSA public key for the SSH server. For detailed information, refer to "Configuring an SSH Client" on page 64.

Configure the public key of the SSH client on the SSH server, and specify the public key name as Switch001

```
[3Com] rsa peer-public-key Switch001
RSA public key view: return to System View with "peer-public-key end".
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[3Com-rsa-key-code] 3047
[3Com-rsa-key-code] 0240
[3Com-rsa-key-code] C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
[3Com-rsa-key-code] 349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
[3Com-rsa-key-code] 74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
[3Com-rsa-key-code] 074C0CA9
[3Com-rsa-key-code] 0203
[3Com-rsa-key-code] 010001
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[3Com]
```

Assign public key Switch001 to user client001

```
[3Com] ssh user client001 assign rsa-key Switch001
```

If first-time authentication is disabled on the device, it is necessary to configure on the SSH client the RSA public key of the SSH server.

Display the RSA public key on the server.

```
[3Com] display rsa local-key-pair public
=====================================================
Time of Key pair created: 09:04:41  2000/04/04
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
308188
  028180
    C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
    FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
    E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
    5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
    024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
    BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
    C289B7DD 2BE0F7AD
  0203
    010001
<Omitted>
```

2 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.

```
<3Com> system-view
[3Com] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[3Com-Vlan-interface1] quit
```

Generate a RSA key pair

```
[3Com] rsa local-key-pair create
```

Export the generated RSA key pair to a file named Switch001.

```
<3Com> display rsa local-key-pair public

=====================================================
Time of Key pair created: 05:15:04  2006/12/08
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
    349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
    74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
    074C0CA9
  0203
    010001
<Omitted>
```

After the SSH client generates an RSA key pair, it is necessary to configure the RSA public key for the SSH server and finish the SSH server configuration before continuing to configure the SSH client.

Disable first-time authentication on the device.

```
[3Com] undo ssh client first-time
```

If first-time authentication is disabled on the device, it is necessary to configure on the SSH client the RSA public key of the SSH server.

Configure the public key of the SSH server on the SSH client, and specify the public key name as Switch002.

```
[3Com] rsa peer-public-key Switch002
RSA public key view: return to System View with "peer-public-key end".
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[3Com-rsa-key-code] 308188
[3Com-rsa-key-code] 028180
[3Com-rsa-key-code] C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
[3Com-rsa-key-code] FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
[3Com-rsa-key-code] E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
[3Com-rsa-key-code] 5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
[3Com-rsa-key-code] 024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
[3Com-rsa-key-code] BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
[3Com-rsa-key-code] C289B7DD 2BE0F7AD
```

```
[3Com-rsa-key-code] 0203
[3Com-rsa-key-code] 010001
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[3Com]
```

Specify the host public key pair name of the server.

```
[3Com] ssh client 10.165.87.136 assign rsa-key Switch002
```

Establish the SSH connection to server 10.165.87.136.

```
[3Com] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

******************************************************************************
* Copyright(c) 2004-2006 Hangzhou 3Com Technologies Co., Ltd.           *
* Without the owner's prior written consent,                            *
* no decompiling or reverse-switch fabricering shall be allowed.        *
******************************************************************************

<3Com>
```

5 ROUTING OVERVIEW

Overview

Static Routing and Routing Protocols

Static routing

Static routing features zero overhead, simple configuration, and is applicable to simple and stable networks. But it requires human intervention when the network topology changes.

RIP

RIP is easy to configure and is insensitive to CPU and memory, so it is applicable to small and medium sized networks. However, it converges slowly and cannot eliminate route loops completely. In addition, periodic RIP updating multicasts or broadcasts consume many network resources.

OSPF

OSPF is complicated to configure and requires high-performance CPU and memory. It is applicable to medium and large sized networks. OSPF converges fast and can eliminate route loops completely. It supports area partition and provides hierarchical route management.

BGP

BGP runs between ASs. Although complicated to configure, BGP features high reliability, stability, and scalability, has flexible and powerful routing policies and eliminates route loops completely.

Routing Protocols Supported by the 3Com Stackable Switches

Table 22 Routing protocols supported by the 3Com stackable switches

Model\Routing Protocols	RIP	OSPF	BGP
Switch 4500	√	-	-
Switch 5500	√	√	-
Switch 5500Gs	√	√	√

Configuration Example

- *This configuration example uses the Switch 5500G.*
- *For configuration precautions, see the configuration guide and command reference guide of the applicable switch.*

Configuration Task List

Table 23 Configuration task List

Task	Details
Static route configuration	"Static Route Configuration" on page 90
RIP configuration	"RIP Configuration" on page 90
OSPF configuration	"OSPF Configuration" on page 95
BGP configuration	"BGP Configuration" on page 103

Static Route Configuration

Table 24 Configure a static route

Operation	Command	Remarks
Enter system view	**system-view**	-
Configure a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group number*] [**description** *text*]	Required By default, the system can obtain the route to the subnet directly connected to the router.

RIP Configuration

Table 25 RIP configuration tasks

Configuration task		Remarks	Related section
Configuring basic RIP functions	Enabling RIP	Required	"Configuring Basic RIP Functions" on page 91
	Setting the RIP operating status on an interface	Optional	"Setting the RIP operating status on an interface" on page 92
	Specifying a RIP version	Optional	"Specifying the RIP version on an interface" on page 92

Table 25 RIP configuration tasks

Configuration task		Remarks	Related section
Configuring RIP route control	Setting the additional routing metrics of an interface	Optional	"Setting the additional routing metrics of an interface" on page 92
	Configuring RIP route summarization	Optional	"Configuring RIP route summarization" on page 93
	Disabling the receiving of host routes	Optional	"Disabling the router from receiving host routes" on page 93
	Configuring RIP to filter incoming/outgoing routes	Optional	"Configuring RIP to filter incoming/outgoing routes" on page 93
	Setting RIP preference	Optional	"Setting RIP preference" on page 93
	Enabling load sharing among interfaces	Optional	"Enabling load sharing among RIP interfaces" on page 94
	Configuring RIP to import routes from another protocol	Optional	"Configuring RIP to redistribute routes from another protocol" on page 94
Adjusting and optimizing a RIP network	Configuring RIP timers	Optional	"Configuring RIP timers" on page 94
	Configuring split horizon	Optional	"Configuring split horizon" on page 94
	Configuring RIP-1 packet zero field check	Optional	"Configuring RIP-1 packet zero field check" on page 94
	Setting RIP-2 packet authentication mode	Optional	"Setting RIP-2 packet authentication mode" on page 95
	Configuring RIP to unicast packets	Optional	"Configuring RIP to unicast RIP packets" on page 95

Configuring Basic RIP Functions

Table 26 Enable RIP on the interfaces attached to a specified network segment

Operation	Command	Remarks
Enter system view	**system-view**	-
Enable RIP and enter RIP view	**rip**	Required
Enable RIP on the specified interface	**network** *network-address*	Required Disabled by default.

Setting the RIP operating status on an interface

Table 27 Set the RIP operating status on an interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Enable the interface to receive RIP update packets	**rip input**	Optional By default, all interfaces are allowed to send and receive RIP update packets.
Enable the interface to send RIP update packets	**rip output**	
Enable the interface to receive and send RIP update packets	**rip work**	

Specifying the RIP version on an interface

Table 28 Specify the RIP version on an interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Specify the version of the RIP running on the interface	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	Optional By default, the version of the RIP running on an interface is RIP-1.

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 29 Set additional routing metric

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Set the additional routing metric to be added for incoming RIP routes on this interface	**rip metricin** *value*	Optional By default, the additional routing metric added for incoming routes on an interface is 0.
Set the additional routing metric to be added for outgoing RIP routes on this interface	**rip metricout** *value*	Optional By default, the additional routing metric added for outgoing routes on an interface is 1.

Configuring RIP route summarization

Table 30 Configure RIP route summarization

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Enable RIP-2 automatic route summarization	**summary**	Required By default, RIP-2 automatic route summarization is enabled.

Disabling the router from receiving host routes

Table 31 Disable the router from receiving host routes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Disable the router from receiving host routes	**undo host-route**	Required By default, the router receives host routes.

Configuring RIP to filter incoming/outgoing routes

Table 32 Configure RIP to filter incoming/outgoing routes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Configure RIP to filter incoming routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**	Required By default, RIP does not filter any incoming route. The **gateway** keyword is used to filter the incoming routes advertised from a specified address.
	filter-policy gateway *ip-prefix-name* **import**	
Configure RIP to filter outgoing routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*] [*process-id*]	Required By default, RIP does not filter any outgoing route.
	filter-policy route-policy *route-policy-name* **export**	

Setting RIP preference

Table 33 Set RIP preference

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Set the RIP preference	**preference** *value*	Required The default RIP preference is 100.

Enabling load sharing among RIP interfaces

Table 34 Enable load sharing among RIP interfaces

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Enable load sharing among RIP interfaces	**traffic-share-across-interface**	Required By default, load sharing among RIP interfaces is disabled

Configuring RIP to redistribute routes from another protocol

Table 35 Configure RIP to import routes from another protocol

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Configure a default cost for an incoming route	**default cost** *value*	Optional 1 by default.
Configure RIP to redistribute routes from another protocol	**import-route** *protocol* [*process-id*] [**cost** *value* | **route-policy** *route-policy-name*]*	Required By default, RIP does redistribute any route from other protocols.

Configuring RIP timers

Table 36 Configure RIP timers

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Set the RIP timers	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	Required By default, the Update timer is set 30 seconds and the Timeout timer to 180 seconds.

Configuring split horizon

Table 37 Configure split horizon

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Enable split horizon	**rip split-horizon**	Required Enabled by default.

Configuring RIP-1 packet zero field check

Table 38 Configure RIP-1 packet zero field check

Operation	Command	Remarks
Enter system view	**system-view**	-

Table 38 Configure RIP-1 packet zero field check

Operation	Command	Remarks
Enter RIP view	**rip**	-
Enable the check of the "must be zero" field in RIP-1 packets	**checkzero**	Required Enabled by default.

Setting RIP-2 packet authentication mode

Table 39 Set RIP-2 packet authentication mode

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Set RIP-2 packet authentication mode	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2453** *key-string* | **rfc2082** *key-string key-id* } }	Required 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 40 Configure RIP to unicast RIP packets

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Configure RIP to unicast RIP packets	**peer** *ip-address*	Required When RIP runs on the link that does not support broadcast or multicast, you must configure RIP to unicast RIP packets.

OSPF Configuration

Table 41 OSPF configuration tasks

Configuration task	Remarks	Related section
Basic OSPF configuration	Required	"Basic OSPF configuration" on page 97
OSPF area attribute configuration	Optional	"Configuring OSPF Area Attributes" on page 97

Table 41 OSPF configuration tasks

Configuration task		Remarks	Related section
OSPF network type configuration	Configuring the network type of an OSPF interface	Optional	"Configuring the Network Type of an OSPF Interface" on page 98
	Configuring an NBMA/P2MP neighbor	Optional	"Configuring an NBMA/P2MP Neighbor" on page 98
	Configuring the DR priority on an OSPF interface	Optional	"Configuring the DR Priority on an OSPF Interface" on page 99
OSPF route control	Configuring OSPF route summarization	Optional	"Configuring OSPF Route Summarization" on page 99
	Configuring OSPF to filter received routes	Optional	"Configuring OSPF to Filter Received Routes" on page 99
	Configuring OSPF interface cost	Optional	"Configuring the OSPF Cost on an Interface" on page 100
	Configuring OSPF route priority	Optional	"Configuring OSPF Route Priority" on page 100
	Configuring the maximum number of OSPF ECMP routes	Optional	"Configuring the Maximum Number of OSPF ECMP Routes" on page 100
	Configuring OSPF to redistribute external routes	Optional	"Configuring OSPF to Redistribute External Routes" on page 100

Table 41 OSPF configuration tasks

Configuration task		Remarks	Related section
OSPF network adjustment and optimization	Configuring OSPF timers	Optional	"Configuring OSPF Timers" on page 101
	Configuring the LSA transmission delay	Optional	"Configure the LSA transmission delay" on page 101
	Configuring the SPF calculation interval	Optional	"Configuring the SPF Calculation Interval" on page 102
	Disabling OSPF packet transmission on an interface	Optional	"Disabling OSPF Packet Transmission on an Interface" on page 102
	Configuring OSPF authentication	Optional	"Configuring OSPF Authentication" on page 102
	Configuring the MTU field in DD packets	Optional	"Configuring the MTU Field in DD Packets" on page 103
	Enabling OSPF logging of neighbor state changes	Optional	"Enabling OSPF Logging of Neighbor State Changes" on page 103
	Configuring OSPF network management	Optional	"Configuring OSPF Network Management" on page 103

Basic OSPF configuration

Table 42 Basic OSPF configuration

Operation	Command	Remarks
Enter system view	**system-view**	-
Configure the router ID	**router id** *router-id*	Optional If multiple OSPF processes run on a router, you are recommended to use the **router-id** keyword in the **ospf** command to specify different router IDs for different processes.
Enable OSPF and enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required Enter OSPF view.
Enter OSPF area view	**area** *area-id*	-
Configure the network segments in the area	**network** *ip-address wildcard-mask*	Required By default, an interface does not belong to any area.

Configuring OSPF Area Attributes

Table 43 Configure OSPF area attributes

Operation	Command	Remarks
Enter system view	**system-view**	-

Table 43 Configure OSPF area attributes

Operation	Command	Remarks
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter OSPF area view	**area** *area-id*	-
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** | **no-import-route** | **no-summary**] *	Optional By default, no area is configured as an NSSA area.
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.
Create and configure a virtual link	**vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*] *	Optional For a virtual link to take effect, you need to use this command at both ends of the virtual link and ensure consistent configurations of the **hello**, **dead**, and other parameters at both ends.

Configuring the Network Type of an OSPF Interface

Table 44 Configure the network type of an OSPF interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the network type of the OSPF interface	**ospf network-type** { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** }	Optional By default, the network type of an interface depends on the physical interface.

Configuring an NBMA/P2MP Neighbor

Table 45 Configure NBMA/P2MP neighbor

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Configure an NBMA/P2MP neighbor	**peer** *ip-address* [**dr-priority** *dr-priority*]	Required By default, the priority for the neighbor of an NBMA interface is 1.

Configuring the DR Priority on an OSPF Interface

Table 46 Configure the DR priority on an OSPF interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the DR priority on the OSPF interface	**ospf dr-priority** *priority*	Optional The default DR priority is 1.

Configuring OSPF Route Summarization

Table 47 Configure ABR route summarization

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter area view	**area** *area-id*	-
Enable ABR route summarization	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]	Required This command takes effect only when it is configured on an ABR. By default, this function is disabled on an ABR.

Table 48 Configure ASBR route summarization

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enable ASBR route summarization	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]	Required This command takes effect only when it is configured on an ASBR. By default, summarization of imported routes is disabled.

Configuring OSPF to Filter Received Routes

Table 49 Configure OSPF to filter received routes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure to filter the received routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**	Required By default, OSPF does not filter received routing information.

Configuring the OSPF Cost on an Interface

Table 50 Configure the OSPF cost on an interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the OSPF cost on the interface	**ospf cost** *value*	Optional By default, the interface calculates the OSPF cost according to the current baud rate on it. For a VLAN interface on the switch, a fixed value of 10 is used.

Configuring OSPF Route Priority

Table 51 Configure OSPF route priority

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure OSPF route priority	**preference** [**ase**] *value*	Optional By default, the OSPF route priority is 10 and the priority of OSPF ASE is 150.

Configuring the Maximum Number of OSPF ECMP Routes

Table 52 Configure the maximum number of OSPF ECMP routes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure the maximum number of OSPF ECMP routes	**multi-path-number** *value*	Optional 3 by default.

Configuring OSPF to Redistribute External Routes

Table 53 Configure OSPF to redistribute external routes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure OSPF to redistribute routes from another protocol	**import-route** *protocol* [*process-id*] [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*] *	Required By default, OSPF does not import the routing information of other protocols.
Configure OSPF to filter outgoing routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]	Optional By default, OSPF does not filter advertised routes.

Table 53 Configure OSPF to redistribute external routes

Operation	Command	Remarks
Enable OSPF to import the default route	**default-route-advertise** [**always** | **cost** *value* | **type** *type-value* | **route-policy** *route-policy-name*]*	Optional By default, OSPF does not import the default route.
Configure the default parameters for redistributed routes, including cost, interval, limit, .tag, and type	**default** { **cost** *value* | **interval** *seconds* | **limit** *routes* | **tag** *tag* | **type** *type* } *	Optional These parameters respectively default to: ■ Cost: 1 ■ Interval: 1 (second) ■ Limit: 1000 ■ Tag: 1 ■ Type: 2

Configuring OSPF Timers

Table 54 Configure OSPF timers

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the hello interval on the interface	**ospf timer hello** *seconds*	Optional By default, **p2p** and **broadcast** interfaces send Hello packets every 10 seconds; while **p2mp** and **NBMA** interfaces send Hello packets every 30 seconds.
Configure the poll interval on the NBMA interface	**ospf timer poll** *seconds*	Optional By default, poll packets are sent every 40 seconds.
Configure the dead time of the neighboring router on the interface	**ospf timer dead** *seconds*	Optional 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.
Configure the interval for retransmitting an LSA on an interface	**ospf timer retransmit** *interval*	Optional By default, this interval is five seconds.

Configure the LSA transmission delay

Table 55 Configure the LSA transmission delay

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-

Table 55 Configure the LSA transmission delay

Operation	Command	Remarks
Configure the LSA transmission delay	**ospf trans-delay** *seconds*	Optional By default, the LSA transmission delay is one second.

Configuring the SPF Calculation Interval

Table 56 Configure the SPF calculation interval

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure the SPF calculation interval	**spf-schedule-interval** *interval*	Optional By default, the SPF calculation interval is five seconds.

Disabling OSPF Packet Transmission on an Interface

Table 57 Disable OSPF packet transmission on an interface

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Disable OSPF packet transmission on a specified interface	**silent-interface** *silent-interface-type silent-interface-number*	Optional By default, all the interfaces are allowed to transmit OSPF packets.

Configuring OSPF Authentication

Table 58 Configure OSPF authentication

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter OSPF area view	**area** *area-id*	-
Configure the authentication mode of the OSPF area	**authentication-mode** { **simple** | **md5** }	Required By default, no authentication mode is configured for an area.
Return to OSPF view	**quit**	-
Return to system view	**quit**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the authentication mode of the OSPF interface	**ospf authentication-mode** { **simple** *password* | **md5** *key-id key* }	Optional By default, OSPF packets are not authenticated on an interface.

Configuring the MTU Field in DD Packets

Table 59 Configure to fill the MTU field when an interface transmits DD packets

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet interface view	**interface** *interface-type interface-number*	Required
Enable the interface to fill in the MTU field when transmitting DD packets	**ospf mtu-enable**	Optional 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.

Enabling OSPF Logging of Neighbor State Changes

Table 60 Enable OSPF logging of neighbor state changes

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enable the OSPF logging of neighbor state changes	**log-peer-change**	Required Disabled by default.

Configuring OSPF Network Management

Table 61 Configure OSPF network management (NM)

Operation	Command	Remarks
Enter system view	**system-view**	-
Configure OSPF MIB binding	**ospf mib-binding** *process-id*	Optional By default, OSPF MIB is bound to the first enabled OSPF process.
Enable OSPF Trap sending	**snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**]*	Optional You can configure OSPF to send diversified SNMP TRAP messages and specify a certain OSPF process to send SNMP TRAP messages by process ID.

BGP Configuration

Table 62 BGP configuration tasks

Configuration task	Remarks	Related section
Configuring Basic BGP Functions	Required	"Configuring Basic BGP Functions" on page 104

Table 62 BGP configuration tasks

Configuration task		Remarks	Related section
Configuring the way to advertise/receive routing information	Importing routes	Optional	"Importing Routes" on page 105
	Configuring route aggregation	Optional	"Configuring BGP Route Aggregation" on page 105
	Enabling Default Route Advertising	Optional	"Enabling Default Route Advertising" on page 106
	Configuring route reception filtering policies	Optional	"Configuring route reception filtering policies" on page 106
	Configure route advertisement filtering policies	Optional	"Configure route advertisement filtering policies" on page 107
	Disable BGP-IGP Route Synchronization	Optional	"Disable BGP-IGP Route Synchronization" on page 107
	Configuring BGP Route Dampening	Optional	"Configuring BGP Route Dampening" on page 108
Configuring BGP route attributes		Optional	"Configuring BGP Route Attributes" on page 108
Adjusting and optimizing a BGP network		Optional	"Adjusting and Optimizing a BGP Network" on page 109
Configure a large-scale BGP network	Configuring BGP Peer Group	Required	"Configuring BGP Peer Group" on page 110
	Configuring BGP Community	Required	"Configuring BGP Community" on page 111
	Configuring BGP RR	Optional	"Configuring BGP Route Reflector (RR)" on page 111
	Configuring BGP Confederation	Optional	"Configuring BGP Confederation" on page 112

Configuring Basic BGP Functions

Table 63 Configure basic BGP functions

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Specify the AS number for the BGP peers	**peer** *group-name* **as-number** *as-number*	By default, a peer is not assigned an AS number.
Assign a description string for a BGP peer/a BGP peer group	**peer** { *group-name* | *ip-address* } **description** *description-text*	Optional By default, a peer/a peer group is not assigned a description string.

Table 63 Configure basic BGP functions

Operation	Command	Description
Activate a specified BGP peer	**peer** { *group-name* | *ip-address* } **enable**	Optional By default, a BGP peer is active.
Enable BGP logging	**log-peer-change**	Optional By default, BGP logging is enabled.
Specify the source interface for route update packets	**peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*	Optional By default, the source interface of the optimal route update packets is used as the source interface.
Allow routers that belong to non-directly connected networks to establish EBGP connections.	**peer** *group-name* **ebgp-max-hop** [*hop-count*]	Optional By default, routers that belong to two non-directly connected networks cannot establish EBGP connections. You can configure the maximum hops of EBGP connection by specifying the *hop-count* argument.

Importing Routes

Table 64 Import routes

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	-
Import the default route to the BGP routing table	**default-route imported**	Optional By default, BGP does not import default routes to the BGP routing table.
Import and advertise routing information generated by other protocols.	**import-route** *protocol* [*process-id*] [**med** *med-value* | **route-policy** *route-policy-name*]*	Required By default, BGP does not import nor advertise the routing information generated by other protocols.
Advertise network segment routes to BGP routing table	**network** *network-address* [*mask*] [**route-policy** *route-policy-name*]	Optional By default, BGP does not advertise any network segment routes.

Configuring BGP Route Aggregation

Table 65 Configure BGP route aggregation

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.

Table 65 Configure BGP route aggregation

Operation		Command	Description
Configure BGP route aggregation	Enable automatic route aggregation	**summary**	Required By default, routes are not aggregated.
	Enable manual route aggregation	**aggregate** *ip-address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*	

Enabling Default Route Advertising

Table 66 Enable default rout advertising

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Enable default route advertising	**peer** *group-name* **default-route-advertise** [**route-policy** *route-policy-name*]	Required By default, a BGP router does not send default routes to a specified peer/peer group.

Configuring route reception filtering policies

Table 67 Configure route reception filtering policies

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Configure the global route reception filtering policy	**filter-policy** { *acl-number* | **gateway** *ip-prefix-name* **| ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**	Required By default, the incoming routing information is not filtered.
Reference a routing policy to filter routes from a peer/peer group	**peer** { *group-name* | *ip-address* } **route-policy** *policy-name* **import**	Required By default, no route filtering policy is specified for a peer/peer group.

Table 67 Configure route reception filtering policies

Operation		Command	Description
Filter the routing information from a peer/peer group	Reference an ACL to filter BGP routes from a peer/peer group	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**	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.
	Reference an AS path ACL to filter routes from a peer/peer group	**peer** { *group-name* | *ip-address* } **as-path-acl** *acl-number* **import**	
	Reference an IP prefix list to filter routes from a peer/peer group	**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* **import**	

Configure route advertisement filtering policies

Table 68 Configure route advertisement filtering policies

Operation		Command	Description
Enter system view		**system-view**	-
Enter BGP view		**bgp** *as-number*	-
Configure the global route advertisement filtering policy		**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]	Required By default, advertised routes are not filtered.
Reference a routing policy to filter the routes to a peer group		**peer** *group-name* **route-policy** *route-policy-name* **export**	Required By default, no route advertising policy is specified for the routes advertised to a peer group.
Filter the routing information to a peer group	Reference an ACL to filter BGP routes to a peer group	**peer** *group-name* **filter-policy** *acl-number* **export**	Required Not configured by default
	Reference an AS path ACL to filter BGP routes to a peer group	**peer** *group-name* **as-path-acl** *acl-number* **export**	
	Reference an IP prefix list to filter BGP routes to a peer group	**peer** *group-name* **ip-prefix** *ip-prefix-name* **export**	

Disable BGP-IGP Route Synchronization

Table 69 Disable BGP-IGP route synchronization

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-

Table 69 Disable BGP-IGP route synchronization

Operation	Command	Description
Disable BGP-IGP route synchronization	undo synchronization	Required By default, BGP routes and IGP routes are not synchronized.

Configuring BGP Route Dampening

Table 70 Configure BGP route dampening

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Configure BGP route dampening-related parameters	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]	Required By default, route dampening is disabled. Other default route dampening-related parameters are as follows. ■ *half-life-reachable*: 15 (in minutes) ■ *half-life-unreachable*: 15 (in minutes) ■ *reuse*: 750 ■ *suppress*: 2000 ■ *ceiling*: 16,000

Configuring BGP Route Attributes

Table 71 Configure BGP route attributes

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Configure the management preference of the exterior, interior and local routes	**preference** *ebgp-value ibgp-value local-value*	Optional By default, the management preference of the exterior, interior and local routes is 256, 256, and 130.
Set the default local preference	**default local-preference** *value*	Optional By default, the local preference defaults to 100.

Table 71 Configure BGP route attributes

Operation		Command	Description
Configure the MED attribute	Configure the default local MED value	**default med** *med-value*	Optional By default, the *med-value* argument is 0.
	Permit to compare the MED values of the routes coming from the neighbor routers in different ASs.	**compare-different-as-med**	Optional By default, the compare of MED values of the routes coming from the neighbor routers in different ASs is disabled.
Configure the local address as the next hop address when a BGP router advertises a route.		**peer** *group-name* **next-hop-local**	Required 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.
Configure the AS_Path attribute	Configure the number of local AS number occurrences allowed	**peer** { *group-name* | *ip-address* } **allow-as-loop**[*number*]	Optional By default, the number of local AS number occurrences allowed is 1.
	Assign an AS number for a peer group	**peer** *group-name* **as-number** *as-number*	Optional By default, the local AS number is not assigned to a peer group.
	Configure that the BGP update packets only carry the pubic AS number in the AS_Path attribute when a peer sends BGP update packets to BGP peers.	**peer** *group-name* **public-as-only**	Optional By default, a BGP update packet carries the private AS number.

Adjusting and Optimizing a BGP Network

Table 72 Adjust and optimize a BGP network

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-

Table 72 Adjust and optimize a BGP network

Operation		Command	Description
Configure BGP timer	Configure the Keepalive time and Holdtime of BGP.	**timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	Optional By default, the keepalive time is 60 seconds, and holdtime is 180 seconds. The priority of the timer configured by the **timer** command is lower than that of the timer configured by the **peer time** command.
	Configure the Keepalive time and holdtime of a specified peer/peer group.	**peer** { *group-name* | *ip-address* } **timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	
Configure the interval at which a peer group sends the same route update packet		**peer** *group-name* **route-update-interval** *seconds*	Optional By default, the interval at which a peer group sends the same route update packet to IBGP peers is 15 seconds, and to EBGP peers is 30 seconds.
Configure the number of route prefixes that can be learned from a BGP peer/peer group		**peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [{ **alert-only** | **reconnect** *reconnect-time* } | *percentage-value*] *	Optional By default, there is no limit on the number of route prefixes that can be learned from the BGP peer/peer group.
Perform soft refreshment of BGP connection manually		**return**	-
		refresh bgp { **all** | *ip-address* | **group** *group-name* } [**multicast**] { **import** | **export** }	Optional
		system-view	Enter BGP view again
		bgp *as-number*	
Configure BGP to perform MD5 authentication when establishing TCP connection		**peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*	Optional By default, BGP dose not perform MD5 authentication when establishing TCP connection.

Configuring BGP Peer Group

Table 73 Configure BGP peer group

Operation		Command	Description
Enter system view		**system-view**	-
Enter BGP view		**bgp** *as-number*	-
Create an IBGP peer group	Create an IBGP peer group	**group** *group-name* [**internal**]	Optional 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.
	Add a peer to a peer group	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	

Table 73 Configure BGP peer group

Operation		Command	Description
Create an EBGP peer group	Create an EBGP peer group	**group** *group-name* **external**	Optional 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.
	Configure the AS number of a peer group	**peer** *group-name* **as-number** *as-number*	
	Add a peer to a peer group	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	
Create a hybrid EBGP peer group	Create an EBGP peer group	**group** *group-name* **external**	Optional You can add multiple peers to the peer group.
	Add a peer to a peer group	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	
Finish the session with the specified peer/peer group		**peer** { *group-name* | *ip-address* } **shutdown**	Optional

Configuring BGP Community

Table 74 Configure BGP community

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Configure the peers to advertise community attribute to each other	**peer** *group-name* **advertise-community**	Required By default, no community attribute or extended community attribute is advertised to any peer group.
Specify routing policy for the routes exported to the peer group	**peer** *group-name* **route-policy** *route-policy-name* **export**	Required By default, no routing policy is specified for the routes exported to the peer group.

Configuring BGP Route Reflector (RR)

Table 75 Configure BGP RR

Operation	Command	Description
Enter system view	**system-view**	-
Enter BGP view	**bgp** *as-number*	-
Configure the local router as the RR and configure the peer group as the client of the RR	**peer** *group-name* **reflect-client**	Required By default, no RR or its client is configured.
Enable route reflection between clients	**reflect between-clients**	Optional By default, route reflection is enabled between clients.
Configure cluster ID of an RR	**reflector cluster-id** *cluster-id*	Optional By default, an RR uses its own router ID as the cluster ID.

Configuring BGP Confederation

Table 76 Configure BGP confederation

Operation		Command	Description
Enter system view		**system-view**	-
Enter BGP view		**bgp** *as-number*	-
Basic BGP confederation configuration	Configure confederation ID	**confederation id** *as-number*	Required By default, no confederation ID is configured and no sub-AS is configured for a confederation.
	Specify the sub-ASs included in a confederation	**confederation peer-as** *as-number-list*	
Configure the compatibility of a confederation		**confederation nonstandard**	Optional By default, the confederation configured is consistent with the RFC 1965.

Route Policy Configuration

Table 77 Route Policy Configuration

Configuration task		Remarks	Related section
Configure an IP-prefix list	Configuring an ip-prefix list	Optional	"Configuring an ip-prefix list" on page 112
	AS path list configuration	Optional	"AS path list configuration" on page 113
	Community list configuration	Optional	"Community list configuration" on page 113
Define a routing policy	Defining a Routing Policy	Required	"Defining a Routing Policy" on page 113
	Define if-match clauses	Optional	"Define if-match clauses" on page 113
	Define apply clauses	Optional	"Define apply clauses" on page 114

Configuring an ip-prefix list

Table 78 Configure an IPv4 IP-prefix list

Operation	Command	Remarks
Enter system view	**system-view**	-
Configure an IPv4 IP-prefix list	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]	Required By default, no IP-prefix list is specified.

AS path list configuration

Table 79 AS path list configuration

Operation	Command	Description
Enter system view	**system-view**	-
Configure AS path list	**ip as-path-acl** *acl-number* { **permit** | **deny** } *as-regular-expression*	Optional By default, no AS path list is defined

Community list configuration

Table 80 Community list configuration

Operation	Command	Description
Enter system view	**system-view**	-
Configure basic community list	**ip community-list** *basic-comm-list-number* { **permit** | **deny** } [*aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**]*	Optional By default, no BGP community list is defined
Configure advanced community list	**ip community-list** *adv-comm-list-number* { **permit** | **deny** } *comm-regular-expression*	Optional By default, no BGP community list is defined

Defining a Routing Policy

Table 81 Define a routing policy

Operation	Command	Remarks
Enter system view	**system-view**	-
Define a routing policy and enter the routing policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required By default, no routing policy is defined.

Define if-match clauses

Table 82 Define if-match clauses

Operation	Command	Description
Enter system view	**system-view**	-
Enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required
Define a rule to match AS path of BGP routing information	**if-match as-path** *as-path-number*	Optional
Define a rule to match community attributes of BGP routing information	**if-match community** { *basic-community-number* [**whole-match**] | *adv-community-number* }	Optional
Define a rule to match the IP address of routing information	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the address of routing information.

Table 82 Define if-match clauses

Operation	Command	Description
Define a rule to match the routing cost of routing information	**if-match cost** *value*	Optional By default, no matching is performed on the routing cost of routing information.
Define a rule to match the next-hop interface of routing information	**if-match interface** *interface-type interface-number*	Optional By default, no matching is performed on the next-hop interface of routing information.
Define a rule to match the next-hop address of routing information	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the next-hop address of routing information.
Define a rule to match the tag field of OSPF routing information	**if-match tag** *value*	Optional By default, no matching is performed on the tag field of OSPF routing information.

Define apply clauses

Table 83 Define apply clauses

Operation	Command	Description
Enter system view	**system-view**	-
Enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required
Add specified AS number for as-path in BGP routing information	**apply as-path** *as-number-1* [*as-number-2* [*as-number-3* ...]]	Optional
Configure community attributes for BGP routing information	**apply community** { **none** | [*aa:nn*] [**no-export-subconfed** | **no-export** | **no-advertise**]***** [**additive**] }	Optional
Set next hop IP address for routing information	**apply ip next-hop** *ip-address*	Optional
Set local preference of BGP routing information	**apply local-preference** *local-preference*	Optional
Define an action to set the cost of routing information	**apply cost** *value*	Optional By default, no action is defined to set the routing cost of routing information.
Set route cost type for routing information	**apply cost-type** [**internal** | **external**]	Optional
Set route source of BGP routing information	**apply origin** { **igp** | **egp** *as-number* | **incomplete** }	Optional
Define an action to set the tag field of routing information	**apply tag** *value*	Optional By default, no action is defined to set the tag field of OSPF routing information.

Configuration Examples

The following configuration examples use the Switch 5500Gs.

Static Routing Configuration Example

Network requirements

1 Requirement analysis:

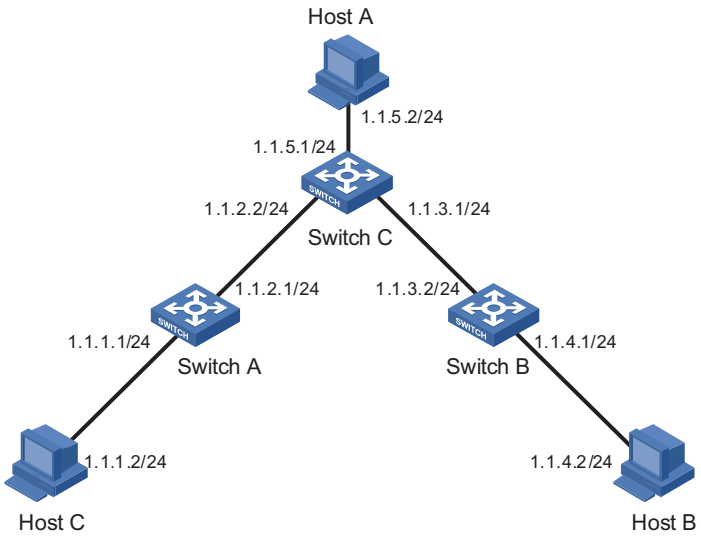
A small company requires any two nodes in its network communicate with each other. The network should be simple and stable. The customer hopes to make the best use of the existing devices that do not support dynamic routing protocols.

Based on the customer requirements and networking environment, configure static routes to realize network interconnection.

2 Network diagram

Figure 51 shows the network diagram.

Figure 51 Network diagram for static route configuration



Configuration procedure

Configure the switches:

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
```

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
```

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
```

Configure the hosts:

Configure the default gateway as 1.1.5.1 on host A (omitted).

Configure the default gateway as 1.1.4.1 on host B (omitted).

Configure the default gateway as 1.1.1.1 on host C (omitted).

Now any two hosts or switches can communicate with each other.

RIP Configuration Examples

Network requirements

1 Requirement analysis:

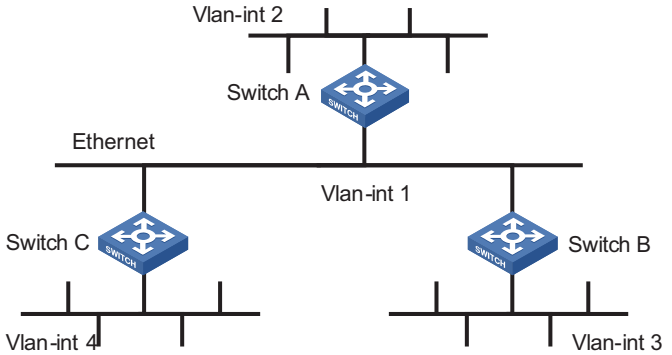
A small company requires any two nodes in its network can communicate with each other. The devices can dynamically adjust to network topology changes.

Based on the customer requirements and networking environment, use RIP to realize network interconnection.

2 Network diagram

Figure 52 shows the network diagram.

Figure 52 Network diagram for RIP configuration



Device	Interface	IP Address	Device	Interface	IP Address
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24
Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

Configuration procedure

Only RIP-related configurations are described below. Before performing the following configurations, make sure that the data link layer works normally and the IP addresses of the VLAN interfaces have been configured.

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.

```
<Switch> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3 Configure Switch C.

Configure RIP.

```
<Switch> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

OSPF DR Configuration Example

Network requirements

1 Requirement analysis

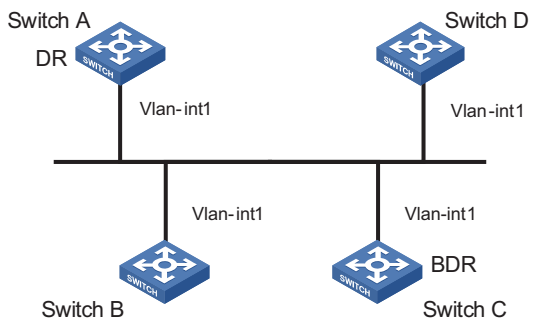
Use OSPF to realize interconnection between devices in a broadcast network. Devices with higher performance should become the DR and BDR to improve network performance. Devices with lower performance are forbidden to take part in DB/BDR election.

Based on the customer requirements and networking environment, assign proper priorities to interfaces.

2 Network diagram

Figure 53 shows the network diagram.

Figure 53 Network diagram for OSPF DR selection



Device	Interface	IP address	Router ID	Interface priority
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1	100
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2	0
Switch C	Vlan-int1	196.1.1.3/24	3.3.3.3	2
Switch D	Vlan-int1	196.1.1.4/24	4.4.4.4	1

Configuration procedure

Configure Switch A.

```
<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.

```
<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.

```
<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
```

Use the **display ospf peer** command to display OSPF neighbors on Switch A. Note that Switch A has three neighbors.

The state of each neighbor is full. This means that Switch A has formed adjacencies with all neighbors. (Switch A and Switch C can act as the DR and BDR only when they establish adjacencies with all the switches in the network.) Switch A acts as the DR, while Switch C acts as the BDR. Any other neighbor is DRother (neither DR nor BDR).

Change the priority of Switch B to 200.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200
```

Use the **display ospf peer** command to display OSPF neighbors on Switch A. Note that the priority of Switch B is 200 now, but it is not the DR.

The DR will be reelected only after the current DR fails to work. Shut down Switch A and use the **display ospf peer** command to display neighbors on Switch D. Note that Switch C that used to be the BDR becomes the DR and Switch B becomes the BDR.

If you shut down and then restart all the switches, Switch B with priority 200 will be elected as the DR and Switch A with priority 100 will be elected as the BDR, because such operation triggers a new round of DR/BDR election.

OSPF Virtual Link Configuration Examples

Network requirements

1 Requirement analysis

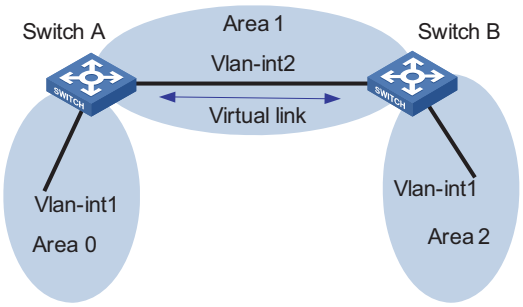
Devices in the network run OSPF to realize interconnection. The network is split into three areas: one backbone area and two non-backbone areas (Area 1 and Area 2). Area 2 has no direct connection to the backbone, and it has to reach the backbone through Area 1. The customer hopes that Area 2 can interconnect with other two areas.

Based on the customer requirements and networking environment, use a virtual link to connect Area 2 to the backbone area.

2 Network diagram

Figure 54 shows the network diagram.

Figure 54 Network diagram for virtual link configuration



Device	Interface	IP address	Router ID
Switch A	Vlan-int1	196.1.1.2/24	1.1.1.1
	Vlan-int2	197.1.1.2/24	-
Switch B	Vlan-int1	152.1.1.1/24	2.2.2.2
	Vlan-int2	197.1.1.1/24	-

Configuration procedure

1 Configure OSPF basic functions

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 197.1.1.2 255.255.255.0
[SwitchA-Vlan-interface2] 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
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 152.1.1.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 197.1.1.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
```

Display the OSPF routing table on Switch A

```
[SwitchA] display ospf routing

                OSPF Process 1 with Router ID 1.1.1.1
                        Routing Tables

Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
196.1.1.0/24              10 Stub 196.1.1.2       1.1.1.1          0.0.0.0
197.1.1.0/24              10 Net  197.1.1.1       2.2.2.2          0.0.0.1

Total Nets: 2
  Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

Since Area2 has no direct connection to Area0, the routing table of RouterA has no route to Area2.

2 Configure a virtual link

Configure Switch A.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Configure Switch B.

```
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 1.1.1.1
[SwitchB-ospf-1-area-0.0.0.1] quit
```

Display the OSPF routing table on Switch A.

```
[SwitchA]display ospf routing

                OSPF Process 1 with Router ID 1.1.1.1
                            Routing Tables

Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
196.1.1.0/24              10 Stub 196.1.1.2       1.1.1.1          0.0.0.0
197.1.1.0/24              10 Net  197.1.1.1       2.2.2.2          0.0.0.1
152.1.1.0/24              20 SNet 197.1.1.1       2.2.2.2          0.0.0.0

Total Nets: 3
  Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

Switch A has learned the route 152.1.1.0/24 to Area2.

BGP Confederation Configuration Example

Network requirements

1 Requirement analysis

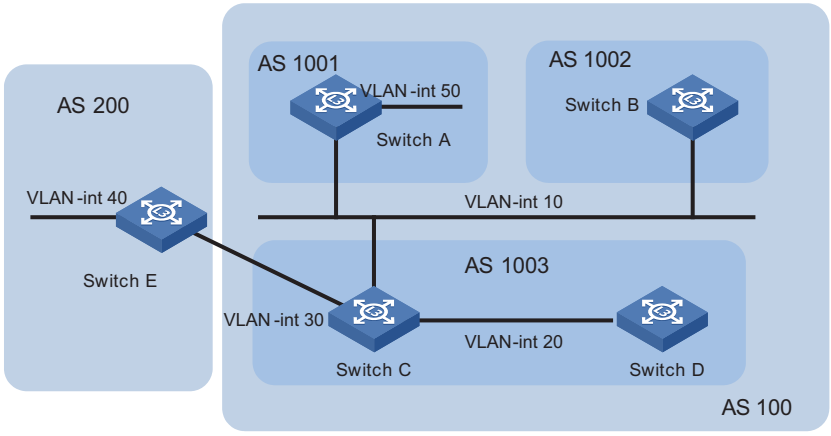
BGP runs in a large AS of a company. As the number of IBGP peers increases rapidly in the AS, more network resources for BGP communication are occupied. The customer hopes to reduce IBGP peers and decrease the CPU and network resources consumption of BGP without affecting device performance.

Based on user requirements, configure a BGP confederation to achieve the goal.

2 Network diagram

Figure 55 shows the network diagram.

Figure 55 Network diagram for BGP AS confederation configuration



Device	Interface	IP address	AS
Switch A	Vlan-int 10	172.68.10.1/24	100
	Vlan-int 50	10.1.1.1/24	
Switch B	Vlan-int 10	172.68.10.2/24	
Switch C	Vlan-int 10	172.68.10.3/24	
	Vlan-int 20	172.68.1.1/24	
	Vlan-int 30	156.10.1.1/24	
Switch D	Vlan-int 20	172.68.1.2/24	
Switch E	Vlan-int 30	156.10.1.2/24	200
	Vlan-int 40	8.1.1.1/24	

3 Configuration plan

- Split AS 100 into three sub-ASs: AS 1001, AS 1002, and AS 1003.
- Run EBGP between AS 1001, AS1002, and AS 1003.
- AS 1001, AS1002, and AS 1003 are fully meshed within themselves by running IBGP.
- Run EBGP between AS 100 and AS 200.

Configuration procedure

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] bgp 1001
[SwitchA-bgp] network 10.1.1.0 255.255.255.0
[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
[SwitchA-bgp] quit
```

Configure Switch B.

```
<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.

```
<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
[SwitchC-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[SwitchC-bgp] group ibgp1003 internal
[SwitchC-bgp] peer 172.68.1.2 group ibgp1003
```

Configure Switch D.

```
<SwitchD> system-view
[SwitchD] bgp 1003
[SwitchD-bgp] confederation id 100
[SwitchD-bgp] group ibgp1003 internal
[SwitchD-bgp] peer 172.68.1.1 group ibgp1003
```

Configure Switch E.

```
<SwitchE> system-view
[SwitchE] bgp 200
[SwitchE-bgp] network 8.1.1.0 255.255.255.0
[SwitchE-bgp] group ebgp100 external
[SwitchE-bgp] peer 156.10.1.1 group ebgp100 as-number 100
[SwitchE-bgp] quit
```

Display the BGP routing table on Switch E.

```
[SwitchE] display bgp routing

Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-Hop        Med        Local-pref Origin Path
------------------------------------------------------------------------------
#^  8.1.1.0/24         0.0.0.0         0          100         IGP
#^  10.1.1.0/24        156.10.1.1      0          100         IGP   100

  Routes total: 2
```

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing

Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed
```

```
    Dest/Mask       Next-Hop      Med      Local-pref  Origin  Path
--------------------------------------------------------------------------------
  I 8.1.1.0/24      156.10.1.2    0        100         IGP     (1003) 200
#^  10.1.1.0/24     0.0.0.0       0        100         IGP

  Routes total: 2
```

The above display shows that sub-AS routing information is advertised only within the confederation. A device in an AS outside of the confederation, such as Switch E, cannot learn the sub-AS routing information within the confederation because it treats the confederation as a single AS.

BGP Route Reflector Configuration Example

Network requirements

1 Requirement analysis

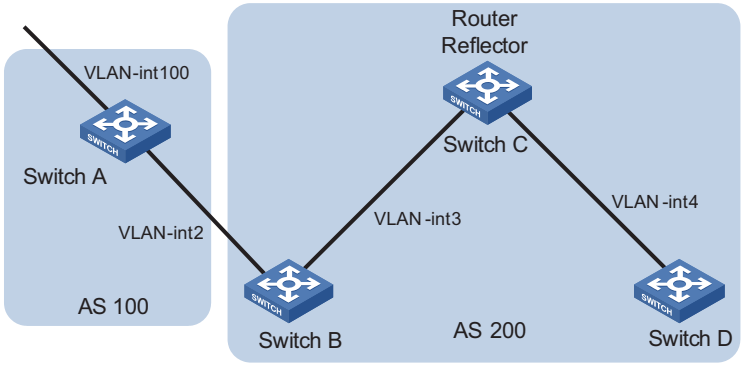
BGP runs in a large AS of a company. As the number of IBGP peers increases rapidly in the AS, more network resources for BGP communication are occupied. The customer hopes to reduce IBGP peers and decrease CPU and network resources consumption of BGP without affecting device performance. In addition, IBGP peers are partially interconnected in the AS.

Based on the requirements and networking environment, configure a BGP route reflector to achieve the goal.

2 Network diagram

Figure 56 shows the network diagram.

Figure 56 Network diagram for BGP route reflector configuration



Device	Interface	IP address	AS
Switch A	Vlan-int 100	1.1.1.1/8	100
	Vlan-int 2	192.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	200
	Vlan-int 3	193.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.1/24	
	Vlan-int 4	194.1.1.1/24	
Switch D	Vlan-int 4	194.1.1.2/24	

3 Configuration plan

- Run EBGP between the peers in AS 100 and AS 200. Advertise 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] 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 the 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 BGP peers.

```
[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 the 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 configure Switch C as the route reflector.

```
[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 the 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 the 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 learned network 1.0.0.0.

Use the **display bgp routing** command to display the BGP routing table on Switch D. Note that Switch D has learned network 1.0.0.0.

BGP Path Selection Configuration Example

Network requirements

1 Requirement analysis

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.

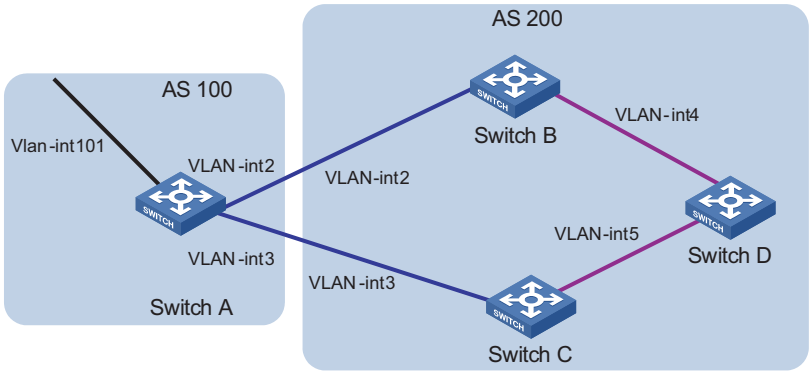
The following give two plans to meet the requirement

- 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

2 Network diagram

Figure 57 shows the network diagram.

Figure 57 Network diagram for BGP path selection



Device	Interface	IP address	AS
Switch A	Vlan-int 101	1.1.1.1/8	100
	Vlan-int 2	192.1.1.1/24	
	Vlan-int 3	193.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	200
	Vlan-int 4	194.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.2/24	
	Vlan-int 5	195.1.1.2/24	
Switch D	Vlan-int 4	194.1.1.1/24	
	Vlan-int 5	195.1.1.1/24	

3 Configuration plan

- Run EBGP between AS 100 and AS 200. Advertise 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 the 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
[SwitchA] interface Vlan-interface 101
[SwitchA-Vlan-interface101] ip address 1.1.1.1 255.0.0.0
[SwitchA-Vlan-interface101] quit
```

Enable BGP.

```
[SwitchA] bgp 100
```

Advertise 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
[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 routes destined for 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 routing updates to the peer group ex193 (the peer 193.1.1.2) and **apply_med_100** to routing updates to the 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 the 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 the 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
```

Enable 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 195.1.1.1 group in
[SwitchC-bgp] peer 194.1.1.2 group in
```

4 Configure Switch D.

Configure the 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
```

Enable 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
[SwitchD-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Enable BGP, create a peer group, and add peers to the peer group.

```
[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 validate the configuration, you need to use the reset bgp all command on all the BGP peers.
- Since the MED attribute of route 1.0.0.0 learned by Switch C is smaller than that learned by Switch B, Switch D selects the route 1.0.0.0 from Switch C.

- If you do not configure MED attribute control on Switch A, setting the local preference attribute for route 1.0.0.0 on Switch C is another choice.

Define ACL 2000 to permit the routes destined for 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
```

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
```

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
```

Apply the routing policy **localpref** to the routing information from the peer 193.1.1.1 (Switch A).

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
```

Since the local preference (200) of the route learned by Switch C is bigger than that learned by Switch B (100), Switch D prefers the route 1.0.0.0 from Switch C. Note that the local preference is not set for route 1.0.0.0 on Switch B, so the route uses the default value 100.

Comprehensive Configuration Example

- *For details about routing protocols, see corresponding configuration guide of products.*
- *For details on using specific commands, see the corresponding command reference guide.*
- *The following examples use the Switch 5500 and Switch 5500G.*

Network Requirements

Requirement Analysis, Network Diagram and Configuration Plan

Requirement analysis

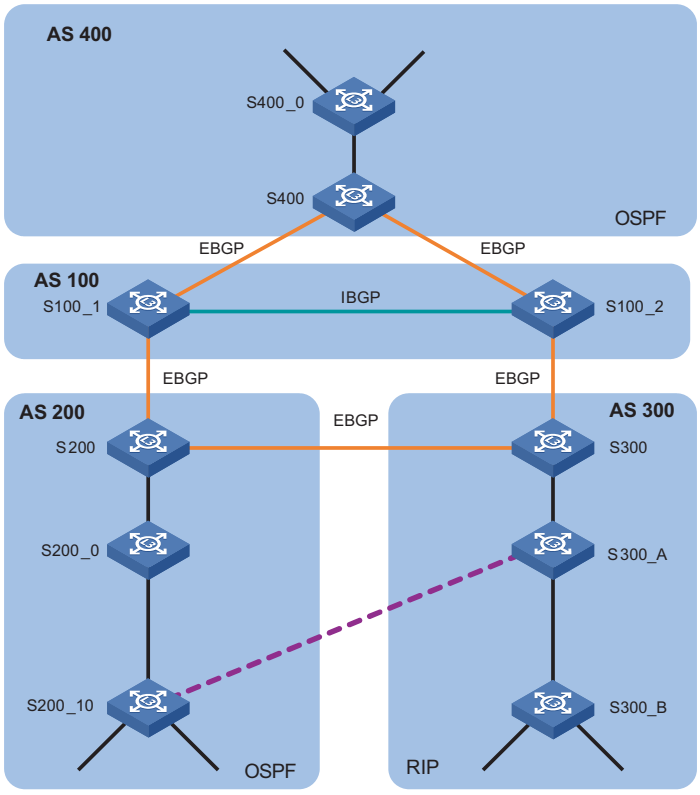
An ISP has four ASs: AS 100, AS 200, AS 300, and AS 400. AS 100 is the core layer. It connects AS 200, AS 300, and AS 400 and forwards data between them. AS 200, AS 300, and AS 400 constitutes the distribution layer. They provide access services for users. The specific requirements are as follows:

- Fast convergence is required for AS 200 and AS 400 because their networks are quite large and complicated.
- The network of AS 300 is small and simple. The devices in the network supports only RIP. Their performances are low and the capacities of routing tables are quite limited.
- Access users in AS 200 require a very reliable network.
- Access users in AS 200, AS 300, and AS 400 are accessible to each other.
- S200_10 in AS 200 is connected with Layer 2 devices.
- S300_B in AS 300 is connected with Layer 2 devices.
- The data forwarding path needs to be controlled when users in AS 400 access AS 200 and AS 300.
- An AS 300 access user is interconnected with the ISP through a single link.

Network diagram

Figure 58 shows the network diagram designed according to the requirements.

Figure 58 Network diagram



Configuration plan

- Run BGP in AS 100 to interconnect with AS 200, AS 300, and AS 400. Use the MED attribute to control the forwarding path.
- Run OSPF in AS 200. The device in AS 200 connecting to AS 100 runs both OSPF and BGP. Use static routes as backup routes to implement link redundancy and improve network reliability. Apply a routing policy when redistributing BGP routes for filtering.

- Run OSPF in AS 400. The device in AS 400 connecting to AS 100 runs both OSPF and BGP. Apply a routing policy when redistributing BGP routes for filtering.
- Run RIPv2 in AS 300. The device in AS 300 connecting to AS 100 runs both RIPv2 and BGP. Apply a routing policy when redistributing BGP routes for filtering.
- AS 300 users use the combination of static routes, RIP, and routing policy to access the ISP.
- Interaction between IGP and BGP is involved in the configuration. Since the default BGP preference is 256, when backup routes exist in the routing table, you need to modify the BGP preference in order to select the primary route as required.

Devices Used for Networking

Table 84 Device model and device name

Model	Device name
7500	S200/S300
5600	S100_1/S100_2/S400
3600	S200_0/S200_10/S300_A/S300_B/ S400_0

- *Either a Switch 7750 or a Switch 5500G can serve as S100_1/S100_2/S400/S200/S300.*
- *You can use other partially layer 3 capable switches as S300_B.*

Routing Protocols and Related Parameters on Devices

Table 85 Routing protocols supported by devices

Device name	Routing protocol	Router ID	AS
S100_1	BGP (IBGP&EBGP)	1.1.1.1	100
S100_2	BGP (IBGP&EBGP)	1.2.1.1	
S200	BGP (EBGP)/OSPF	2.1.1.1	200
S200_0	OSPF	-	
S200_10	OSPF/STATIC		
S300	BGP (EBGP)/RIPv2	3.1.1.1	300
S300_A	RIPv2/STATIC	-	
S300_B	RIPv2		
S400	BGP (EBGP)/OSPF	4.1.1.1	400
S400_0	OSPF	-	

Software Version

Switch 5500 Release V03.02.04

Switch 5500G Release V03.02.04

Switch 7750 Release 3130

Configuration Procedure

Configuration Guide

Table 86 Configuration guide

Configuration task	Description
"Basic Configuration" on page 133	Create VLANs and configure IP addresses for VLAN interfaces
"Basic RIPv2/OSPF/BGP Configuration" on page 133	Basic RIPv2/OSPF/BGP configuration
"RIP, Static Route, and Routing Policy Configuration Example" on page 139	Using a routing policy, configure RIP to advertise route updates but does not receive route updates and use static routing to access the ISP.
"BGP and IGP Interaction Configuration Example" on page 140	IGP and BGP share routes. Apply a routing policy for BGP redistribution to IGP as required
"Route Backup Configuration Example" on page 142	To improve network reliability, run OSPF on the primary link and run static routing on the backup link to realize interconnection
"BGP MED Attribute Configuration Example" on page 143	Apply a routing policy to change the MED attribute of routes to control the forwarding path

Basic Configuration

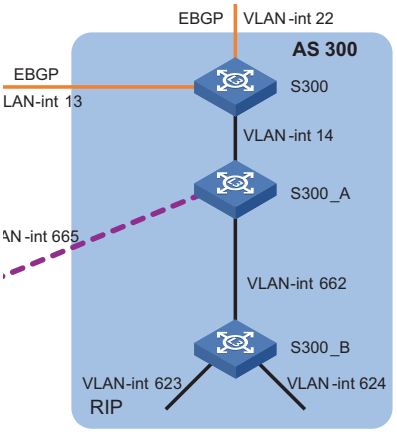
Creating VLANs and configuring IP addresses for VLAN interfaces are omitted here, refer to "Displaying the Whole Configuration on Devices" on page 147 for related information.

Basic RIPv2/OSPF/BGP Configuration

Basic RIPv2 configuration

Figure 59 shows the relevant network diagram of AS 300.

Figure 59 Network diagram for RIPv2 configuration



Device	Interface	IP address
S300	Vlan-int 14	206.1.4.2/24
S300_A	Vlan-int 14	206.1.4.1/24
	Vlan-int 662	166.1.2.1/24
	Vlan-int 665	166.1.5.2/24
S300_B	Vlan-int 662	166.1.2.2/24
	Vlan-int 623	162.1.3.1/24
	Vlan-int 624	162.1.4.1/24

- Configure S300.

Run RIP on the interface with the IP address 206.1.4.0.

```
<S300> system-view
[S300] rip
[S300-rip] network 206.1.4.0
```

Disable RIPv2 route summarization.

```
[S300-rip] undo summary
[S300-rip] quit
```

Run RIPv2 on VLAN-interface 14.

```
[S300] interface vlan-interface 14
[S300-Vlan-interface14] rip version 2
[S300-Vlan-interface14] quit
```

- Configure S300_A.

Run RIP on the interfaces on networks 206.1.4.0 and 166.1.0.0.

```
<S300_A> system-view
[S300_A] rip
[S300_A-rip] network 206.1.4.0
[S300_A-rip] network 166.1.0.0
```

Disable RIPv2 route summarization.

```
[S300_A-rip] undo summary
[S300_A-rip] quit
```

Run RIPv2 on VLAN-interface 14 and VLAN-interface 662.

```
[S300_A] interface vlan-interface 14
[S300_A-Vlan-interface14] rip version 2
[S300_A-Vlan-interface14] quit
[S300_A] interface vlan-interface 662
[S300_A-Vlan-interface662] rip version 2
[S300_A-Vlan-interface662] quit
```

- Configure S300_B.

Run RIP on the interfaces connected to networks 162.1.0.0 and 166.1.0.0.

```
<S300_B> system-view
[S300_B] rip
[S300_B-rip] network 162.1.0.0
[S300_B-rip] network 166.1.0.0
```

Disable RIPv2 route summarization.

```
[S300_B-rip] undo summary
[S300_B-rip] quit
```

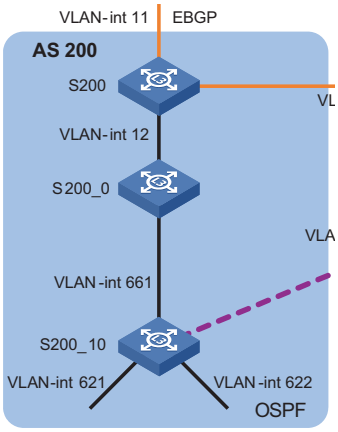
Run RIPv2 on VLAN-interface 623, VLAN-interface 624, and VLAN-interface 662.

```
[S300_B] interface vlan-interface 623
[S300_B-Vlan-interface623] rip version 2
[S300_B-Vlan-interface623] quit
[S300_B] interface vlan-interface 624
[S300_B-Vlan-interface624] rip version 2
[S300_B-Vlan-interface624] quit
[S300_B] interface vlan-interface 662
[S300_B-Vlan-interface662] rip version 2
[S300_B-Vlan-interface662] quit
```

Basic OSPF configuration

Figure 60 shows the relevant network diagram of AS 200.

Figure 60 Network diagram for OSPF configuration



Device	Interface	IP address	Area
S200	Vlan-int 12	206.1.2.3/24	0
S200_0	Vlan-int 12	206.1.2.1/24	0
	Vlan-int 661	166.1.1.1/24	10
S200_10	Vlan-int 661	166.1.1.2/24	10
	Vlan-int 621	162.1.1.1/24	10
	Vlan-int 622	162.1.2.1/24	10

- Configure S200.

Run OSPF on the interface connected to network 206.1.2.0/24 and specify its area ID as 0.

```
<S200> system-view
[S200] ospf
[S200-ospf-1] area 0
[S200-ospf-1-area-0.0.0.0] network 206.1.2.0 0.0.0.255
```

- Configure S200_0.

Run OSPF on the interface connected to network 206.1.2.0/24 and specify its area ID as 0.

```
<S200_0> system-view
[S200_0] ospf
[S200_0-ospf-1] area 0
```

```
[S200_0-ospf-1-area-0.0.0.0] network 206.1.2.0 0.0.0.255
[S200_0-ospf-1-area-0.0.0.0] quit
```

Run OSPF on the interface connected to network 166.1.1.0/24 and specify its area ID as 10.

```
[S200_0-ospf-1] area 10
[S200_0-ospf-1-area-0.0.0.10] network 166.1.1.0 0.0.0.255
```

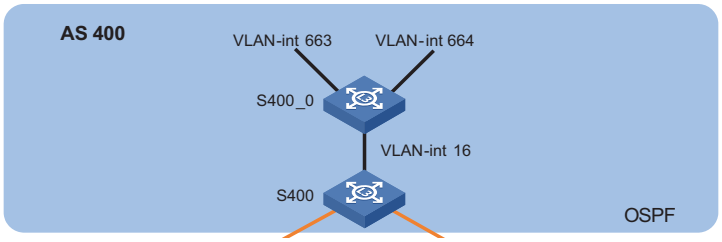
- Configure S200_10.

Run OSPF on interfaces connected to networks 162.1.1.0/24, 162.1.2.0/24, and 166.1.1.0/24 and specify their area ID as 10.

```
<S200_10> system-view
[S200_10] ospf
[S200_10-ospf-1] area 10
[S200_10-ospf-1-area-0.0.0.10] network 162.1.1.0 0.0.0.255
[S200_10-ospf-1-area-0.0.0.10] network 162.1.2.0 0.0.0.255
[S200_10-ospf-1-area-0.0.0.10] network 166.1.1.0 0.0.0.255
```

Figure 61 shows the network diagram of AS 400.

Figure 61 Network diagram for AS 400 configuration



Device	Interface	IP address	Area
S400	Vlan-int 16	206.1.6.3/24	0
S400_0	Vlan-int 16	206.1.6.1/24	0
	Vlan-int 663	166.1.3.1/24	0.0.1.44
	Vlan-int 664	166.1.4.1/24	0.0.1.44

- Configure S400.

Run OSPF on the interface connected to network 206.1.6.0/24 and specify its area ID as 0.

```
<S400> system-view
[S400] ospf
[S400-ospf-1] area 0
[S400-ospf-1-area-0.0.0.0] network 206.1.6.0 0.0.0.255
```

- Configure S400_0.

Run OSPF on the interface connected to network 206.1.6.0/24 and specify its area ID as 0.

```
<S400_0> system-view
[S400_0] ospf
[S400_0-ospf-1] area 0
[S400_0-ospf-1-area-0.0.0.0] network 206.1.6.0 0.0.0.255
[S400_0-ospf-1-area-0.0.0.0] quit
```

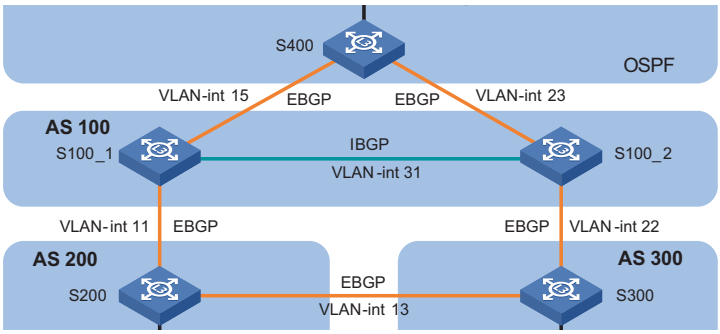
Run OSPF on interfaces connected to networks 166.1.3.0/24 and 166.1.4.0/24 and specify their area ID as 0.0.1.44.

```
[S400_0-ospf-1] area 0.0.1.44
[S400_0-ospf-1-area-0.0.1.44] network 166.1.3.0 0.0.0.255
[S400_0-ospf-1-area-0.0.1.44] network 166.1.4.0 0.0.0.255
```

Basic BGP configuration

Figure 62 shows the relevant network diagram.

Figure 62 Network diagram for BGP configuration



Device	Interface	IP address	Router ID	AS
S100_1	Vlan-int 11	196.1.1.1/24	1.1.1.1	100
	Vlan-int 15	196.1.3.1/24		
	Vlan-int 31	196.3.1.1/24		
S100_2	Vlan-int 22	196.2.2.1/24	1.2.1.1	
	Vlan-int 23	196.2.3.2/24		
	Vlan-int 31	196.3.1.2/24		
S200	Vlan-int 11	196.1.1.3/24	2.1.1.1	200
	Vlan-int 13	206.1.3.3/24		
S300	Vlan-int 22	196.2.2.2/24	3.1.1.1	300
	Vlan-int 13	206.1.3.2/24		
S400	Vlan-int 15	196.1.3.3/24	4.1.1.1	400
	Vlan-int 23	196.2.3.3/24		

- Configure S100_1.

Configure the router ID of S100_1 as 1.1.1.1.

```
<S100_1> system-view
[S100_1] router id 1.1.1.1
```

Enable BGP and specify the local AS number as 100.

```
[S100_1] bgp 100
```

Create IBGP peer group 100 and EBGP peer groups 200 and 400.

```
[S100_1-bgp] group 100 internal
[S100_1-bgp] group 200 external
[S100_1-bgp] group 400 external
```

Add peer 196.3.1.2 in AS 100 into peer group 100; Add peer 196.1.1.3 in AS 200 into peer group 200; Add peer 196.1.3.3 in AS 400 into peer group 400.

```
[S100_1-bgp] peer 196.3.1.2 group 100
[S100_1-bgp] peer 196.1.1.3 group 200 as-number 200
[S100_1-bgp] peer 196.1.3.3 group 400 as-number 400
```

Advertise networks 196.1.3.0, 196.3.1.0, and 196.1.1.0.

```
[S100_1-bgp] network 196.1.3.0
[S100_1-bgp] network 196.3.1.0
[S100_1-bgp] network 196.1.1.0
```

Set the preferences of EBGP routes, IBGP routes, and local routes to 200.

```
[S100_1-bgp] preference 200 200 200
```

- Configure S100_2.

Configure the router ID of S200_2 as 1.2.1.1.

```
<S100_2> system-view
[S100_2] router id 1.2.1.1
```

Enable BGP and specify the local AS number as 100.

```
[S100_2] bgp 100
```

Create IBGP peer group 100 and EBGP peer groups 300 and 400.

```
[S100_2-bgp] group 100 internal
[S100_2-bgp] group 300 external
[S100_2-bgp] group 400 external
```

Add peer 196.3.1.1 in AS 100 into peer group 100; Add peer 196.2.2.2 in AS 300 into peer group 300; Add peer 196.2.3.3 in AS 400 into peer group 400.

```
[S100_2-bgp] peer 196.3.1.1 group 100
[S100_2-bgp] peer 196.2.2.2 group 300 as-number 300
[S100_2-bgp] peer 196.2.3.3 group 400 as-number 400
```

Advertise networks 196.2.2.0, 196.2.3.0, and 196.3.1.0.

```
[S100_2-bgp] network 196.2.2.0
[S100_2-bgp] network 196.2.3.0
[S100_2-bgp] network 196.3.1.0
```

Set the preferences of EBGP routes, IBGP routes, and local routes to 200.

```
[S100_2-bgp] preference 200 200 200
```

- Configure S200.

Configure the router ID of S200 as 2.1.1.1.

```
<S200> system-view
[S200] router id 2.1.1.1
```

Enable BGP and specify the local AS number as 200.

```
[S200] bgp 200
```

Create EBGP peer groups 100 and 300.

```
[S200-bgp] group 100 external
[S200-bgp] group 300 external
```

Add peer 196.1.1.1 in AS 100 into peer group 100; Add peer 206.1.3.2 in AS 300 into peer group 300.

```
[S200-bgp] peer 196.1.1.1 group 100 as-number 100
[S200-bgp] peer 206.1.3.2 group 300 as-number 300
```

Advertise networks 192.1.1.0 and 206.1.3.0.

```
[S200-bgp] network 192.1.1.0
[S200-bgp] network 206.1.3.0
```

Set the preferences of EBGP routes, IBGP routes, and local routes to 200.

```
[S200-bgp] preference 200 200 200
```

- Configure S300.

Configure the router ID of S300 as 3.1.1.1.

```
<S300> system-view
[S300] router id 3.1.1.1
```

Enable BGP and specify the local AS number as 300.

```
[S300] bgp 300
```

Create EBGP peer groups 100 and 200.

```
[S300-bgp] group 100 external
[S300-bgp] group 200 external
```

Add peer 196.2.2.1 in AS 100 into peer group 100; Add peer 206.1.3.3 in AS 200 into peer group 200.

```
[S300-bgp] peer 196.2.2.1 group 100 as-number 100
[S300-bgp] peer 206.1.3.3 group 200 as-number 200
```

Advertise networks 206.1.3.0 and 196.2.2.0.

```
[S300-bgp] network 206.1.3.0
[S300-bgp] network 196.2.2.0
```

Set the preferences of EBGP routes, IBGP routes, and local routes to 200.

```
[S300-bgp] preference 200 200 200
```

- Configure S400.

Configure the router ID of S400 as 4.1.1.1.

```
<S400> system-view
[S400] router id 4.1.1.1
```

Enable BGP and specify the local AS number as 400.

```
[S400] bgp 400
```

Create EBGP peer groups 100_1 and 100_2.

```
[S400-bgp] group 100_1 external
[S400-bgp] group 100_2 external
```

Add peer 196.1.3.1 in AS 100 into peer group 100_1; Add peer 196.2.3.2 in AS 100 into peer group 100_2.

```
[S400-bgp] peer 196.1.3.1 group 100_1 as-number 100
[S400-bgp] peer 196.2.3.2 group 100_2 as-number 100
```

Advertise networks 196.1.3.0 and 196.2.3.0.

```
[S400-bgp] network 196.1.3.0
[S400-bgp] network 196.2.3.0
```

Set the preferences of EBGP routes, IBGP routes, and local routes to 200.

```
[S400-bgp] preference 200 200 200
```

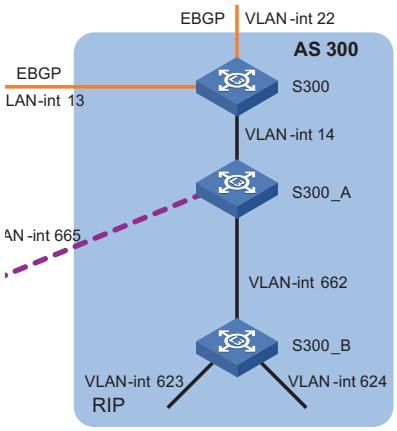
RIP, Static Route, and Routing Policy Configuration Example

Network requirements

As shown in Figure 63, RIPv2 runs on S300_A/S300_B. To control the number of routes learned by S300_B through RIP, allow S300_B to advertise routes to S300_A and forbid S300_B to receive routes advertised by S300_A. Packets from S300_B to S300_A are forwarded through the default route.

Network diagram

Figure 63 Network diagram for RIP, static route, and routing policy configuration



Device	Interface	IP address
S300_A	Vlan-int 662	166.1.2.1/24
S300_B	Vlan-int 662	166.1.2.2/24
	Vlan-int 623	162.1.3.1/24
	Vlan-int 624	162.1.4.1/24

Configuration procedure

Create ACL 2000 and deny all packets.

```
<S300_B> system-view
[S300_B] acl number 2000
[S300_B-acl-basic-2000] rule deny source any
[S300_B-acl-basic-2000] quit
```

Apply ACL 2000 to incoming RIP routes.

```
[S300_B] rip
[S300_B-rip] filter-policy 2000 import
```

Configure a default route and specify the next-hop IP address as 166.1.2.1.

```
[S300_B] ip route-static 0.0.0.0 0.0.0.0 166.1.2.1 preference 60
```

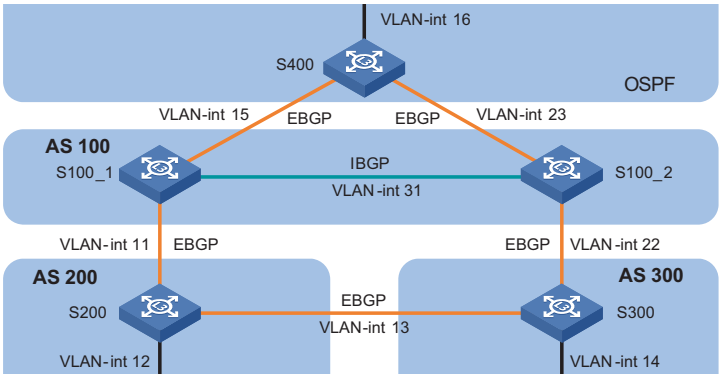
BGP and IGP Interaction Configuration Example

Network requirements

As shown in Figure 64, OSPF and BGP run on S400/S200. RIPv2 and BGP run on S300. To ensure that devices in each AS can learn network topologies of other ASs, configure interaction between IGP and BGP to share routes. When redistributing routes from IGP to BGP, apply a routing policy to redistribute routes with IP prefixes 162.1.1.0/24, 162.1.2.0/24, 162.1.3.0/24, 162.1.4.0/24, 166.1.3.0/24, and 166.1.4.0/24 only.

Network diagram

Figure 64 Network diagram for BGP and IGP interaction



Configuration procedure

- Configure interaction between IGP and BGP on S200.

Redistribute OSPF routes into BGP.

```
<S200> system-view
[S200] bgp 200
[S200-bgp] import-route ospf 1
[S200-bgp] quit
```

Define a prefix list named **ospf_import** and permit the routes with IP prefixes 162.1.3.0/24, 162.1.4.0/24, 166.1.3.0/24, or 166.1.4.0/24.

```
[S200] ip ip-prefix ospf_import index 10 permit 162.1.3.0 24
[S200] ip ip-prefix ospf_import index 20 permit 162.1.4.0 24
[S200] ip ip-prefix ospf_import index 30 permit 166.1.4.0 24
[S200] ip ip-prefix ospf_import index 40 permit 166.1.3.0 24
```

Create a routing policy named **ospf_import** with the match mode as permit. Define an if-match clause to permit routes whose destination addresses match IP prefix list **ospf_import**.

```
[S200] route-policy ospf_import permit node 10
[S200-route-policy] if-match ip-prefix ospf_import
[S200-route-policy] quit
```

Redistribute BGP routes into OSPF and apply routing policy **ospf_import**.

```
[S200] ospf
[S200-ospf-1] import-route bgp route-policy ospf_import
```

- Configure interaction between IGP and BGP on S300.

Redistribute RIP routes into BGP.

```
<S300> system-view
[S300] bgp 300
[S300-bgp] import-route rip
[S300-bgp] quit
```

Define a prefix list named **rip_import** and permit the routes with IP prefixes 162.1.1.0/24, 162.1.2.0/24, 166.1.3.0/24, and 166.1.4.0/24.

```
[S300] ip ip-prefix rip_import index 10 permit 162.1.1.0 24
[S300] ip ip-prefix rip_import index 20 permit 162.1.2.0 24
[S300] ip ip-prefix rip_import index 30 permit 166.1.3.0 24
[S300] ip ip-prefix rip_import index 40 permit 166.1.4.0 24
```

Create a routing policy named **rip_import** with the matching mode as permit. Define an if-match clause to permit routes whose destination addresses match IP prefix list **rip_import**.

```
[S300] route-policy rip_import permit node 10
[S300-route-policy] if-match ip-prefix rip_import
[S300-route-policy] quit
```

Redistribute BGP routes into RIP and apply routing policy **rip_import**.

```
[S300] rip
[S300-rip] import-route bgp route-policy rip_import
```

- Configure interaction between IGP and BGP on S400.

Redistribute OSPF routes into BGP.

```
<S400> system-view
[S400] bgp 400
[S400-bgp] import-route ospf 1
[S400-bgp] quit
```

Define a prefix list named **ospf_import** and permit the routes with IP prefixes 162.1.1.0/24, 162.1.2.0/24, 162.1.3.0/24, and 162.1.4.0/24.

```
[S400] ip ip-prefix ospf_import index 10 permit 162.1.1.0 24
[S400] ip ip-prefix ospf_import index 20 permit 162.1.2.0 24
[S400] ip ip-prefix ospf_import index 30 permit 162.1.3.0 24
[S400] ip ip-prefix ospf_import index 40 permit 162.1.4.0 24
```

Create a routing policy named **ospf_import** with the match mode as permit. Define an if-match clause to permit the routes whose destination addresses match IP prefix list **ospf_import**.

```
[S400] route-policy ospf_import permit node 10
[S400-route-policy] if-match ip-prefix ospf_import
[S400-route-policy] quit
```

Redistribute BGP routes into OSPF and apply the routing policy named ospf_import.

```
[S400] ospf
[S400-ospf-1] import-route bgp route-policy ospf_import
```

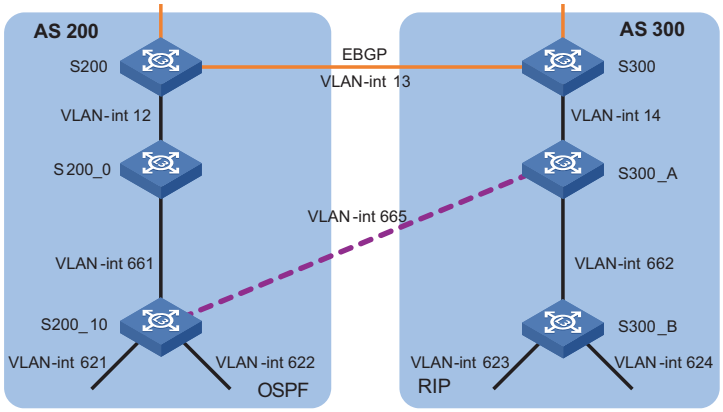
Route Backup Configuration Example

Network requirements

As shown in Figure 65, implement route backup on S200_10. Run OSPF between S200_10 and S200_0. The OSPF route is the primary route. Configure a default route between S200_10 and S300_A. This route is the backup route. When the primary route cannot work, the device switches to the backup route automatically. When the primary route becomes feasible, the device switches to the primary route automatically. To achieve the route backup of S200_10, configure a static route to S200_10 on S300_A and redistribute this route into RIPv2.

Network diagram

Figure 65 Network diagram for route backup



Device	Interface	IP address	AS
S300_A	Vlan-int 665	166.1.5.2/24	300
S200_10	Vlan-int 665	166.1.5.1/24	200
	Vlan-int 621	162.1.1.1/24	
	Vlan-int 622	162.1.2.1/24	

Configuration procedure

Configure a default route on S200_10 and specify the next-hop IP address as 166.1.5.2. Set the default preference to 200.

```
<S200_10> system-view
[S200_10] ip route-static 0.0.0.0 0.0.0.0 166.1.5.2 preference 200
```

Configure a static route on S300_A and specify the destination IP addresses as 162.1.1.0/24 and 162.1.2.0/24. Specify the next-hop IP address as 166.1.5.1 and the default preference to 200.

```
<S300_A> system-view
[S300_A] ip route-static 162.1.1.0 255.255.255.0 166.1.5.1 preference 200
[S300_A] ip route-static 162.1.2.0 255.255.255.0 166.1.5.1 preference 200
```

Redistribute the static route into RIP.

```
[S300_A] rip
[S300_A-rip] import-route static
```

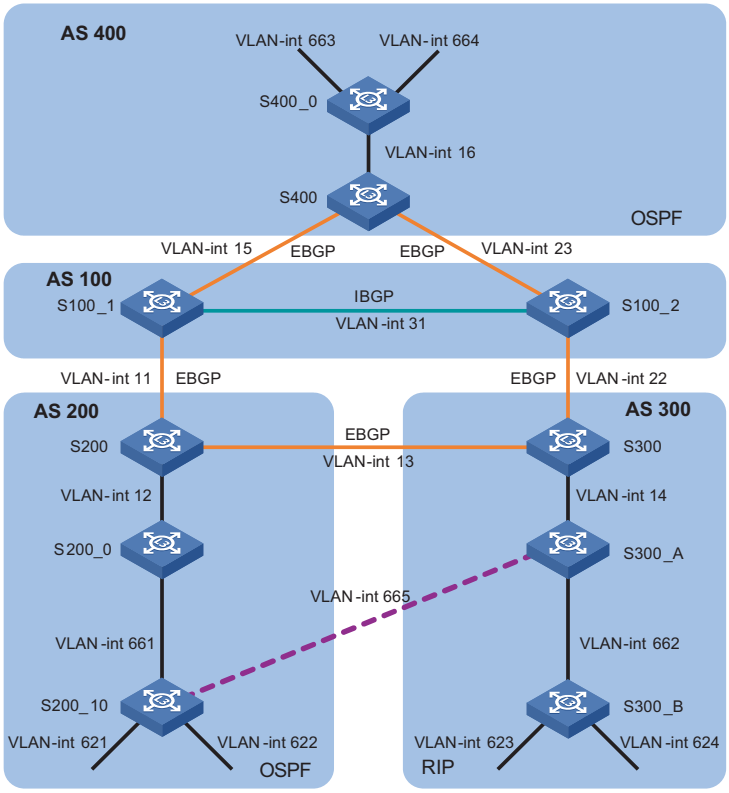
BGP MED Attribute Configuration Example

Network requirements

As shown in Figure 66, S100_1 forwards packets from S400 to S200_10. S100_2 forwards packets from S400 to S300_B. Modify the MED value to achieve this goal.

Network diagram

Figure 66 Network diagram for MED attribute configuration



Device	Interface	IP address	AS
S200_10	Vlan-int 621	162.1.1.1/24	200
	Vlan-int 622	162.1.2.1/24	
S300_B	Vlan-int 623	162.1.3.1/24	300
	Vlan-int 624	162.1.4.1/24	
S400_0	Vlan-int 663	166.1.3.1/24	400
	Vlan-int 664	166.1.4.1/24	

Configuration procedure

- Configure S100_1.

Define a prefix list named **as200_1** and permit the route with IP prefix 162.1.1.0/24.

```
<S100_1> system-view
[S100_1] ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
```

Define a prefix list named **as200_2** and permit the route with IP prefix 162.1.2.0/24.

```
[S100_1] ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
```

Define a prefix list named **as300_1** and permit the route with IP prefix 162.1.3.0/24.

```
[S100_1] ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
```

Define a prefix list named **as300_2** and permit the route with IP prefix 162.1.4.0/24.

```
[S100_1] ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
```

Define a prefix list named **other** and permit all the routes.

```
[S100_1] ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
```

Create a routing policy named **as200**, and specify node 10 with the permit matching mode in the routing policy. Set the MED value of the route matching prefix list **as200_1** to 100.

```
[S100_1] route-policy as200 permit node 10
[S100_1-route-policy] if-match ip-prefix as200_1
[S100_1-route-policy] apply cost 100
[S100_1-route-policy] quit
```

Create node 20 with the matching mode as permit in routing policy **as200**. Set the MED value of the route matching prefix list **as200_2** to 100

```
[S100_1] route-policy as200 permit node 20
[S100_1-route-policy] if-match ip-prefix as200_2
[S100_1-route-policy] apply cost 100
[S100_1-route-policy] quit
```

Create node 30 with the permit matching mode in routing policy **as200**. Set the MED value of the route matching prefix list **as300_1** to 200.

```
[S100_1] route-policy as200 permit node 30
[S100_1-route-policy] if-match ip-prefix as300_1
[S100_1-route-policy] apply cost 200
[S100_1-route-policy] quit
```

Create node 40 with the permit matching mode in routing policy **as200**. Set the MED value of the route matching prefix list **as300_2** to 200.

```
[S100_1] route-policy as200 permit node 40
[S100_1-route-policy] if-match ip-prefix as300_2
[S100_1-route-policy] apply cost 200
[S100_1-route-policy] quit
```

Create node 50 with the permit matching mode in routing policy **as200**. Permit all the routes.

```
[S100_1] route-policy as200 permit node 50
[S100_1-route-policy] if-match ip-prefix other
[S100_1-route-policy] quit
```

Apply the routing policy **as200** to the routes outgoing to peer group 400 (the peer 196.1.3.3).

```
[S100_1] bgp 100
[S100_1-bgp] peer 400 route-policy as200 export
```

- Configure S100_2.

Define a prefix list named **as200_1** and permit the route with IP prefix 162.1.1.0/24.

```
<S100_2> system-view
[S100_2] ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
```

Define a prefix list named **as200_2** and permit the route with IP prefix 162.1.2.0/24.

```
[S100_2] ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
```

Define a prefix list named **as300_1** and permit the route with IP prefix 162.1.3.0/24.

```
[S100_2] ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
```

Define a prefix list named **as300_2** and permit the route with IP prefix 162.1.4.0/24.

```
[S100_2] ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
```

Define a prefix list named **other** and permit all the routes.

```
[S100_2] ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
```

Create a routing policy named **as300**. Configure the node number as 10 and the matching mode as permit. Set the MED value of the route matching prefix list **as200_1** to 200.

```
[S100_2] route-policy as300 permit node 10
[S100_2-route-policy] if-match ip-prefix as200_1
[S100_2-route-policy] apply cost 200
[S100_2-route-policy] quit
```

Create node 20 with the permit matching mode in routing policy **as300**. Set the MED value of the route matching prefix list **as200_2** to 200.

```
[S100_2] route-policy as300 permit node 20
[S100_2-route-policy] if-match ip-prefix as200_2
[S100_2-route-policy] apply cost 200
[S100_2-route-policy] quit
```

Create node 30 with the permit matching mode in routing policy **as300**. Set the MED value of the route matching prefix list **as300_1** to 100.

```
[S100_2] route-policy as300 permit node 30
[S100_2-route-policy] if-match ip-prefix as300_1
[S100_2-route-policy] apply cost 100
[S100_2-route-policy] quit
```

Create node 40 with the permit matching mode in routing policy **as300**. Set the MED value of the route matching prefix list **as300_2** to 100.

```
[S100_2] route-policy as300 permit node 40
[S100_2-route-policy] if-match ip-prefix as300_2
[S100_2-route-policy] apply cost 100
[S100_2-route-policy] quit
```

Create node 50 with the permit matching mode in routing policy **as300** and permit all routes.

```
[S100_2] route-policy as300 permit node 50
[S100_2-route-policy] if-match ip-prefix other
[S100_2-route-policy] quit
```

Apply routing policy **as300** to the routes outgoing to peer group 400 (peer 196.2.3.3).

```
[S100_2] bgp 100
[S100_2-bgp] peer 400 route-policy as300 export
```

Displaying the Whole Configuration on Devices

Displaying the Whole Configuration on Devices

S100_1

```
<S100_1> display current-configuration
#
 sysname S100_1
#
 router id 1.1.1.1
#
....
#
vlan 11
#
vlan 15
#
vlan 31
#
interface Vlan-interface11
 ip address 196.1.1.1 255.255.255.0
#
interface Vlan-interface15
 ip address 196.1.3.1 255.255.255.0
#
interface Vlan-interface31
 ip address 196.3.1.1 255.255.255.0
#
...
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
interface NULL0
#
bgp 100
 network 196.1.3.0
 network 196.3.1.0
 network 196.1.1.0
 undo synchronization
 group 100 internal
 peer 196.3.1.2 group 100
 group 200 external
 peer 196.1.1.3 group 200 as-number 200
 group 400 external
 peer 400 route-policy as200 export
 peer 196.1.3.3 group 400 as-number 400
 preference 200 200 200
#
route-policy as200 permit node 10
 if-match ip-prefix as200_1
 apply cost 100
route-policy as200 permit node 20
 if-match ip-prefix as200_2
 apply cost 100
route-policy as200 permit node 30
```

```
 if-match ip-prefix as300_1
 apply cost 200
route-policy as200 permit node 40
 if-match ip-prefix as300_2
 apply cost 200
route-policy as200 permit node 50
 if-match ip-prefix other
#
 ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
 ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
 ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
 ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
 ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
#
...
```

S100_2

```
<S100_2> display current-configuration
#
 sysname S100_2
#
 router id 1.2.1.1
#
......
#
vlan 22
#
vlan 23
#
vlan 31
#
interface Vlan-interface22
 ip address 196.2.2.1 255.255.255.0
#
interface Vlan-interface23
 ip address 196.2.3.2 255.255.255.0
#
interface Vlan-interface31
 ip address 196.3.1.2 255.255.255.0
#
...
#
interface Cascade1/2/1
#
interface Cascade1/2/2
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
interface NULL0
#
bgp 100
 network 196.2.2.0
 network 196.2.3.0
 network 196.3.1.0
 undo synchronization
 group 100 internal
```

```
 peer 196.3.1.1 group 100
 group 300 external
 peer 196.2.2.2 group 300 as-number 300
 group 400 external
 peer 400 route-policy as300 export
 peer 196.2.3.3 group 400 as-number 400
 preference 200 200 200
#
route-policy as300 permit node 10
 if-match ip-prefix as200_1
 apply cost 200
route-policy as300 permit node 20
 if-match ip-prefix as200_2
 apply cost 200
route-policy as300 permit node 30
 if-match ip-prefix as300_1
 apply cost 100
route-policy as300 permit node 40
 if-match ip-prefix as300_2
 apply cost 100
route-policy as300 permit node 50
 if-match ip-prefix other
#
 ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
 ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
 ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
 ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
 ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
#
.....
```

S200

```
<S200> display current-configuration
#
 sysname S200
#
......
#
 router id 2.1.1.1
#
...........
#
vlan 11
#
vlan 12
#
vlan 13
#
interface Vlan-interface11
 ip address 196.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 206.1.2.3 255.255.255.0
#
interface Vlan-interface13
 ip address 206.1.3.3 255.255.255.0
#
```

```
.......
#
bgp 200
 network 192.1.1.0
 network 206.1.3.0
 import-route ospf 1
 undo synchronization
 group 100 external
 peer 196.1.1.1 group 100 as-number 100
 group 300 external
 peer 206.1.3.2 group 300 as-number 300
 preference 200 200 200
#
ospf 1
 import-route bgp route-policy ospf_import
 area 0.0.0.0
  network 206.1.2.0 0.0.0.255
#
route-policy ospf_import permit node 10
 if-match ip-prefix ospf_import
#
 ip ip-prefix ospf_import index 10 permit 162.1.3.0 24
 ip ip-prefix ospf_import index 20 permit 162.1.4.0 24
 ip ip-prefix ospf_import index 30 permit 166.1.4.0 24
 ip ip-prefix ospf_import index 40 permit 166.1.3.0 24
#
......
```

S200_0

```
<S200_0> display current-configuration
#
 sysname S200_0
#
.......
#
vlan 12
#
vlan 661
#
interface Vlan-interface12
 ip address 206.1.2.1 255.255.255.0
#
interface Vlan-interface661
 ip address 166.1.1.1 255.255.255.0
#
.......
#
ospf 1
 area 0.0.0.10
  network 166.1.1.0 0.0.0.255
 #
 area 0.0.0.0
  network 206.1.2.0 0.0.0.255
#
..........
```

S200_10

```
<S200_10> display current-configuration
#
 sysname S200_10
#
.......
#
vlan 621 to 622
#
vlan 661
#
vlan 665
#
interface Vlan-interface621
 ip address 162.1.1.1 255.255.255.0
#
interface Vlan-interface622
 ip address 162.1.2.1 255.255.255.0
#
interface Vlan-interface661
 ip address 166.1.1.2 255.255.255.0
#
interface Vlan-interface665
 ip address 166.1.5.1 255.255.255.0
#
.........
#
ospf 1
 area 0.0.0.10
  network 162.1.1.0 0.0.0.255
  network 162.1.2.0 0.0.0.255
  network 166.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 166.1.5.2 preference 200
#
.........
```

S300

```
<S300> display current-configuration
#
 sysname S300
#
router id 3.1.1.1
#
.....
#
vlan 13
#
vlan 14
#
vlan 22
#
interface Vlan-interface13
 ip address 206.1.3.2 255.255.255.0
#
interface Vlan-interface14
 ip address 206.1.4.2 255.255.255.0
```

```
 rip version 2 multicast
#
interface Vlan-interface22
 ip address 196.2.2.2 255.255.255.0
#
......
#
bgp 300
 network 206.1.3.0
 network 196.2.2.0
 import-route rip
 undo synchronization
 group 100 external
 peer 196.2.2.1 group 100 as-number 100
 group 200 external
 peer 206.1.3.3 group 200 as-number 200
 preference 200 200 200
#
rip
 undo summary
 network 206.1.4.0
 import-route bgp route-policy rip_import
#
route-policy rip_import permit node 10
 if-match ip-prefix rip_import
#
 ip ip-prefix rip_import index 10 permit 162.1.1.0 24
 ip ip-prefix rip_import index 20 permit 162.1.2.0 24
 ip ip-prefix rip_import index 30 permit 166.1.3.0 24
 ip ip-prefix rip_import index 40 permit 166.1.4.0 24
#
.........
```

S300_A

```
<S300_A> display current-configuration
#
 sysname S300_A
#
......
#
vlan 14
#
vlan 662
#
vlan 665
#
interface Vlan-interface14
 ip address 206.1.4.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface662
 ip address 166.1.2.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface665
 ip address 166.1.5.2 255.255.255.0
#
```

```
......
#
rip
 undo summary
 network 206.1.4.0
 network 166.1.0.0
 import-route static
#
ip route-static 162.1.1.0 255.255.255.0 166.1.5.1 preference 200
 ip route-static 162.1.2.0 255.255.255.0 166.1.5.1 preference 200
#
.........
```

S300_B

```
<S300_B> display current-configuration
#
 sysname S300_B
#
......
#
acl number 2000
 rule 5 deny
#
......
#
vlan 623
#
vlan 624
#
vlan 662
#
interface Vlan-interface623
 ip address 162.1.3.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface624
 ip address 162.1.4.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface662
 ip address 166.1.2.2 255.255.255.0
 rip version 2 multicast
#
......
#
rip
 undo summary
 network 166.1.0.0
 network 162.1.0.0
 filter-policy 2000 import
#
 ip route-static 0.0.0.0 0.0.0.0 166.1.2.1 preference 60
#
......
```

S400

```
<S400> display current-configuration
#
 sysname S400
#
 router id 4.1.1.1
#
......
#
vlan 15 to 16
#
vlan 23
#
interface Vlan-interface15
 ip address 196.1.3.3 255.255.255.0
#
interface Vlan-interface16
 ip address 206.1.6.3 255.255.255.0
#
interface Vlan-interface23
 ip address 196.2.3.3 255.255.255.0
#
......
#
interface Cascade1/2/1
#
interface Cascade1/2/2
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
interface NULL0
#
bgp 400
 network 196.1.3.0
 network 196.2.3.0
 import-route ospf 1
 undo synchronization
 group 100_1 external
 peer 196.1.3.1 group 100_1 as-number 100
 group 100_2 external
 peer 196.2.3.2 group 100_2 as-number 100
 preference 200 200 200
#
ospf 1
 import-route bgp route-policy ospf_import
 area 0.0.0.0
  network 206.1.6.0 0.0.0.255
#
route-policy ospf_import permit node 10
 if-match ip-prefix ospf_import
#
 ip as-path-acl 1 permit ^100 200$
 ip as-path-acl 2 permit ^100 300$
#
 ip ip-prefix ospf_import index 10 permit 162.1.1.0 24
 ip ip-prefix ospf_import index 20 permit 162.1.2.0 24
```

```
 ip ip-prefix ospf_import index 30 permit 162.1.3.0 24
 ip ip-prefix ospf_import index 40 permit 162.1.4.0 24
#
.....
```

S400_0

```
<S400_0> display current-configuration
#
 sysname S400_0
#
.........
#
vlan 16
#
vlan 663 to 664
#
.........
#
interface Vlan-interface16
 ip address 206.1.6.1 255.255.255.0
#
interface Vlan-interface663
 ip address 166.1.3.1 255.255.255.0
#
interface Vlan-interface664
 ip address 166.1.4.1 255.255.255.0
#
.........
#
ospf 1
 area 0.0.1.44
  network 166.1.3.0 0.0.0.255
  network 166.1.4.0 0.0.0.255
 #
 area 0.0.0.0
  network 206.1.6.0 0.0.0.255
#
.........
```

Verifying the Configuration

Verifying the Configuration of Routing Policy and Static Routes

```
<S300_B> display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost  Nexthop     Interface
0.0.0.0/0            STATIC   60    0     166.1.2.1   Vlan-interface662
127.0.0.0/8          DIRECT   0     0     127.0.0.1   InLoopBack0
127.0.0.1/32         DIRECT   0     0       127.0.0.1   InLoopBack0
162.1.3.0/24         DIRECT   0     0     162.1.3.1   Vlan-interface623
162.1.3.1/32         DIRECT   0     0     127.0.0.1   InLoopBack0
162.1.4.0/24         DIRECT   0     0     162.1.4.1   Vlan-interface624
162.1.4.1/32         DIRECT   0     0     127.0.0.1   InLoopBack0
166.1.2.0/24         DIRECT   0     0     166.1.2.2   Vlan-interface662
166.1.2.2/32         DIRECT   0     0     127.0.0.1   InLoopBack0
<S300_B> tracert -a 162.1.3.1 166.1.4.1
 traceroute to 166.1.4.1(166.1.4.1) 30 hops max,40 bytes packet
 1 166.1.2.1 18 ms  3 ms  3 ms
```

```
 2 206.1.4.2 9 ms  4 ms  4 ms
 3 196.2.2.1 9 ms  9 ms  18 ms
 4 196.2.3.3 6 ms  3 ms  4 ms
 5 206.1.6.1 14 ms  4 ms  3 ms
```

Verifying the BGP and IGP Interaction Configuration

```
<S400_0> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol  Pre  Cost    Nexthop      Interface
127.0.0.0/8       DIRECT    0     0       127.0.0.1    InLoopBack0
127.0.0.1/32      DIRECT    0     0       127.0.0.1    InLoopBack0
162.1.1.0/24      O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.2.0/24      O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.3.0/24      O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.4.0/24      O_ASE     150   1       206.1.6.3    Vlan-interface16
166.1.3.0/24      DIRECT    0     0       166.1.3.1    Vlan-interface663
166.1.3.1/32      DIRECT    0     0       127.0.0.1    InLoopBack0
166.1.4.0/24      DIRECT    0     0       166.1.4.1    Vlan-interface664
166.1.4.1/32      DIRECT    0     0       127.0.0.1    InLoopBack0
192.168.0.0/24    DIRECT    0     0      192.168.0.30 Vlan-interface1
192.168.0.30/32   DIRECT    0     0      127.0.0.1    InLoopBack0
206.1.6.0/24      DIRECT     0     0      206.1.6.1    Vlan-interface16
206.1.6.1/32      DIRECT     0     0      127.0.0.1    InLoopBack0
<S300_A> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost    Nexthop         Interface
127.0.0.0/8       DIRECT    0    0       127.0.0.1       InLoopBack0
127.0.0.1/32      DIRECT    0    0       127.0.0.1       InLoopBack0
162.1.1.0/24      RIP       100  1       206.1.4.2       Vlan-interface14
162.1.2.0/24      RIP       100  1       206.1.4.2       Vlan-interface14
162.1.3.0/24      RIP       100  1       166.1.2.2       Vlan-interface662
162.1.4.0/24      RIP       100  1       166.1.2.2       Vlan-interface662
166.1.2.0/24      DIRECT   0    0      166.1.2.1       Vlan-interface662
166.1.2.1/32      DIRECT   0    0      127.0.0.1       InLoopBack0
166.1.3.0/24      RIP      100  1       206.1.4.2       Vlan-interface14
166.1.4.0/24      RIP       100  1       206.1.4.2       Vlan-interface14
166.1.5.0/24      DIRECT   0    0      166.1.5.2       Vlan-interface665
166.1.5.2/32      DIRECT   0    0      127.0.0.1       InLoopBack0
206.1.4.0/24      DIRECT   0    0      206.1.4.1       Vlan-interface14
206.1.4.1/32      DIRECT   0    0       127.0.0.1       InLoopBack0
<S200_10> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0         STATIC    200  0      166.1.5.2   Vlan-interface665
127.0.0.0/8       DIRECT    0    0      127.0.0.1   InLoopBack0
127.0.0.1/32      DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.1.0/24      DIRECT    0    0      162.1.1.1   Vlan-interface621
162.1.1.1/32      DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.2.0/24      DIRECT    0    0     162.1.2.1    Vlan-interface622
162.1.2.1/32      DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.3.0/24      O_ASE     150  1      166.1.1.1   Vlan-interface661
162.1.4.0/24      O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.1.0/24      DIRECT    0    0      166.1.1.2   Vlan-interface661
166.1.1.2/32      DIRECT    0    0      127.0.0.1   InLoopBack0
166.1.3.0/24      O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.4.0/24      O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.5.0/24      DIRECT    0    0      166.1.5.1   Vlan-interface665
166.1.5.1/32      DIRECT    0    0      127.0.0.1   InLoopBack0
206.1.2.0/24      OSPF      10   20     166.1.1.1   Vlan-interface661
```

Verifying the Route Backup Configuration

Verify the primary route is installed into the routing table

```
<S200_10> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0         STATIC    200  0      166.1.5.2   Vlan-interface665
```

```
127.0.0.0/8        DIRECT    0    0      127.0.0.1   InLoopBack0
127.0.0.1/32      DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.1.0/24       DIRECT    0    0      162.1.1.1   Vlan-interface621
162.1.1.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.2.0/24       DIRECT    0    0     162.1.2.1    Vlan-interface622
162.1.2.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
162.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.1.0/24       DIRECT    0    0      166.1.1.2   Vlan-interface661
166.1.1.2/32       DIRECT    0    0      127.0.0.1   InLoopBack0
166.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.5.0/24       DIRECT    0    0      166.1.5.1   Vlan-interface665
166.1.5.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
206.1.2.0/24       OSPF      10   20     166.1.1.1   Vlan-interface661
<S200_10> tracert -a 162.1.1.1 166.1.3.1
 traceroute to  166.1.3.1(166.1.3.1) 30 hops max,40 bytes packet
 1 166.1.1.1 10 ms  3 ms  3 ms
 2 206.1.2.3 13 ms  3 ms  5 ms
 3 196.1.1.1 9 ms  3 ms  4 ms
 4 196.1.3.3 12 ms  3 ms  3 ms
 5 206.1.6.1 14 ms  5 ms  3 ms
```

Verify the backup route is installed into the routing table after the primary one fails

```
<S200_10> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0           STATIC   200  0      166.1.5.2    Vlan-interface665
127.0.0.0/8         DIRECT   0    0        127.0.0.1    InLoopBack0
127.0.0.1/32        DIRECT   0    0      127.0.0.1    InLoopBack0
162.1.1.0/24        DIRECT   0    0      162.1.1.1     Vlan-interface621
162.1.1.1/32        DIRECT   0    0      127.0.0.1     InLoopBack0
162.1.2.0/24        DIRECT   0    0      162.1.2.1     Vlan-interface622
162.1.2.1/32        DIRECT   0    0      127.0.0.1     InLoopBack0
166.1.5.0/24        DIRECT   0    0      166.1.5.1     Vlan-interface665
166.1.5.1/32        DIRECT   0    0      127.0.0.1    InLoopBack0
<S200_10> tracert -a 162.1.1.1 166.1.3.1
 traceroute to  166.1.3.1(166.1.3.1) 30 hops max,40 bytes packet
 1 166.1.5.2 11 ms  3 ms  4 ms
 2 206.1.4.2 13 ms  3 ms  4 ms
 3 196.2.2.1 13 ms  3 ms  6 ms
 4 196.2.3.3 11 ms  3 ms  4 ms
 5 206.1.6.1 12 ms  3 ms  4 ms
```

Verifying the MED Attribute Configuration

Trace the packet forwarding path when the default MED is used

```
<S400_0> tracert -a 166.1.3.1 162.1.1.1
 traceroute to  162.1.1.1(162.1.1.1) 30 hops max,40 bytes packet
 1 206.1.6.3 11 ms  3 ms  7 ms
 2 196.1.3.1 10 ms  3 ms  8 ms
 3 196.1.1.3 8 ms  3 ms  3 ms
 4 206.1.2.1 13 ms  4 ms  3 ms
 5 166.1.1.2 13 ms  4 ms  3 ms
<S400_0> tracert -a 166.1.3.1 162.1.3.1
 traceroute to  162.1.3.1(162.1.3.1) 30 hops max,40 bytes packet
 1 206.1.6.3 11 ms  3 ms  3 ms
 2 196.1.3.1 14 ms  4 ms  5 ms
 3 196.3.1.2 10 ms  8 ms  17 ms
 4 196.2.2.2 14 ms  3 ms  3 ms
 5 206.1.4.1 13 ms  3 ms  3 ms
 6 166.1.2.2 13 ms  3 ms  4 ms
```

Trace the packet forwarding path after the MED is modified

Create AS path ACL 1 and permit the routes whose AS_PATH starts with 100 and ends with 200.

```
[S400] ip as-path-acl 1 permit ^100 200$
```

Display the routes that match AS path ACL 1.

```
<S400> display bgp routing as-path-acl 1

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
    Dest/Mask        Next-Hop      Med   Local-pref   Origin      Path
------------------------------------------------------------------------
#^  162.1.1.0/24      196.1.3.1        100    100           INC      100 200
#   162.1.1.0/24      196.2.3.2        200    100           INC      100 200
#^  162.1.2.0/24      196.1.3.1        100    100           INC      100 200
#   162.1.2.0/24      196.2.3.2        200    100           INC      100 200
#^  166.1.1.0/24      196.1.3.1        0        100           INC    100 200
#   166.1.1.0/24      196.2.3.2        0        100           INC    100 200
#^  206.1.3.0         196.1.3.1      0      100           IGP       100 200
```

Create AS path ACL 2 and permit the routes whose AS_PATH starts with 100 and ends with 300.

```
[S400] ip as-path-acl 2 permit ^100 300$
```

Display the routes that match AS path ACL 2.

```
<S400> display bgp routing as-path-acl 2

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
    Dest/Mask         Next-Hop       Med       Local-pref   Origin     Path
------------------------------------------------------------------------
#^  162.1.3.0/24     196.2.3.2      100       100            INC      100 300
#   162.1.3.0/24     196.1.3.1      200       100            INC      100 300
#^  162.1.4.0/24     196.2.3.2      100       100            INC      100 300
#   162.1.4.0/24     196.1.3.1      200       100            INC      100 300
#^  166.1.2.0/24     196.1.3.1      0         100            INC      100 300
#   166.1.2.0/24     196.2.3.2      0         100            INC      100 300
#^  166.1.5.0/24     196.1.3.1      0         100            INC      100 300
#   166.1.5.0/24     196.2.3.2      0         100            INC      100 300
#   206.1.3.0         196.2.3.2      0         100           IGP      100 300
<S400_0> tracert -a 166.1.3.1 162.1.1.1
 traceroute to  162.1.1.1(162.1.1.1) 30 hops max,40 bytes packet
 1 206.1.6.3 9 ms  4 ms  3 ms
 2 196.1.3.1 13 ms  4 ms  3 ms
 3 196.1.1.3 14 ms  4 ms  3 ms
 4 206.1.2.1 12 ms  3 ms  3 ms
 5 166.1.1.2 13 ms  4 ms  3 ms
<S400_0> tracert -a 166.1.3.1 162.1.3.1
 traceroute to  162.1.3.1(162.1.3.1) 30 hops max,40 bytes packet
 1 206.1.6.3 10 ms  4 ms  3 ms
 2 196.2.3.2 13 ms  3 ms  5 ms
 3 196.2.2.2 12 ms  5 ms  3 ms
 4 206.1.4.1 12 ms  4 ms  3 ms
 5 166.1.2.2 14 ms  3 ms  5 ms
```

Precautions

In the configuration and verification process, pay attention to the following points:

- Disable the Fabric function before enabling BGP on Fabric-capable devices.

- To achieve the configuration goal, you are recommended to set the BGP preference to 200. For devices with static routes configured, set a preference for the static routes as required.
- On S300_A, the backup route (static route) cannot be switched to the primary RIP route automatically, so you need to delete the backup route manually and then add it again.
- Since the routing policy is applied when BGP routes are redistributed into IGP, some route entries may not be redistributed, so you are recommended to use the **tracert -a** /**ping -a** command to verify the configuration in the source address mode.

6 MULTICAST PROTOCOL CONFIGURATION EXAMPLES

Keywords:

IGMP, PIM-DM, PIM-SM, MSDP, IGMP Snooping

Abstract:

This document introduces how to configure multicast functions on Ethernet switches in practical networking, based on three typical networking scenarios:

1. Deployment of PIM-DM plus IGMP, with and without IGMP Snooping respectively. Multicast group filtering in IGMP and IGMP Snooping is mainly described for this scenario.
2. Deployment of PIM-SM plus IGMP, with and without IGMP Snooping respectively. Simulated joining is mainly described for this scenario.
3. IGMP Snooping only. The function of dropping unknown multicast data is mainly described for this scenario.

Acronyms:

Internet Group Management Protocol (IGMP), Internet Group Management Protocol Snooping (IGMP Snooping), Protocol Independent Multicast Dense Mode (PIM-DM), Protocol Independent Multicast Sparse Mode (PIM-SM), Multicast Source Discovery Protocol (MSDP)

Multicast Protocol Overview

Different from unicast and broadcast, the multicast technique efficiently addresses the issue of point-to-multipoint data transmission. By allowing high-efficiency point-to-multipoint data transmission, multicast greatly saves network bandwidth and reduces network load.

With the multicast technique, service providers can easily provide new value-added services, such as live Webcasting, Web TV, distance learning, Telemedicine, Web radio, real-time videoconferencing, and other bandwidth- and time-critical information services.

IGMP

As a TCP/IP protocol responsible for IP multicast group membership management, the Internet Group Management Protocol (IGMP) is used by IP hosts to establish and maintain their multicast group memberships to the immediately neighboring multicast router.

PIM

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging unicast routing tables generated by static routing or any unicast routing protocol, such as the Routing Information Protocol (RIP), Open Shortest Path First

(OSPF), Intermediate System to Intermediate System (IS-IS), or the Border Gateway Protocol (BGP). PIM uses the unicast routing table to perform reverse path forwarding (RPF) check in multicast forwarding.

Based on the forwarding mechanism, PIM falls into two modes:

- PIM-DM
- PIM-SM

PIM-DM is a type of dense mode multicast protocol. It uses the "push mode" for multicast forwarding, suitable for small-sized networks with densely distributed multicast group members.

PIM-SM is a type of sparse mode multicast protocol. It uses the "pull mode" for multicast forwarding, suitable for large- and medium-sized networks with sparsely and widely distributed multicast group members.

IGMP Snooping

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast monitoring mechanism that runs on Layer 2 devices to manage and control multicast groups. By analyzing received IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and MAC multicast groups and forwards multicast data based on these mappings.

MSDP

The Multicast Source Discovery Protocol (MSDP) is an inter-domain multicast solution for the interconnection of PIM-SM domains. It is used to discover the multicast source information in other PIM-SM domains.

Within a PIM-SM domain, the multicast source registers only with the local rendezvous point (RP). Therefore, the RP knows all the sources within its own domain only. If there is a mechanism that allows RPs of different PIM-SM domains to share their multicast source information, the information of active sources in other domains can be delivered to the local receivers, so that multicast data can be transmitted among different domains. MSDP achieves this objective. By setting up MSDP peering relationships among RPs of different domains, MSDP propagates source active (SA) messages, which carry multicast source information, between these MSDP peers, thus to allow multicast traffic to flow between different PIM-SM domains.

IGMP Proxy

When a multicast routing protocol (such as PIM-DM) is deployed on a large network, many stub networks may exist. It is tedious work to configure and manage these stub networks.

To minimize the workload of such configuration and management without affecting the multicast connections of the multicast networks, you can configure IGMP Proxy on a Layer 3 switch in the edge networks, so that the Layer 3 switch forwards the IGMP join and IGMP leave messages sent by the hosts attached to it. After the IGMP Proxy configuration, the Layer 3 switch is no longer a PIM neighbor to the external network; instead, it is a host. The Layer 3 switch receives multicast data for a multicast group only when a member of that group is directly attached to it.

Support of Multicast Features

Multicast features supported by the 3Com series Ethernet switches vary with device models. For details, see the corresponding configuration guide. Table 87 lists the multicast features supported by 3Com series Ethernet switches.

Table 87 Multicast features supported by the 3Com stackable switches

Model\Feature	IGMP Snooping	IGMP	PIM	MSDP
Switch 5500	●	●	●	●
Switch 4500	●	-	-	-
Switch 5500Gs	●	●	●	●
Switch 4200	●	-	-	-
Switch 4200G	●	-	-	-
Switch 4210	●	-	-	-
E352&E328	●	-	-	-
E126	●	-	-	-
S3152P	●	-	-	-
E152	●	-	-	-

Configuration Guidance

The following configuration guidance describes the configuration of multicast features based on the implementations on the Switch 5500Gs Ethernet switches. For more information, see the corresponding configuration guide.

Configuring IGMP Snooping

Complete these tasks to configure IGMP Snooping:

Configuration task	Remarks
"Enabling IGMP Snooping" on page 163	Required
"Configuring IGMP-Snooping timers" on page 163	Optional
"Configuring fast leave processing" on page 164	Optional
"Configuring a multicast group filter" on page 164	Optional
"Configuring the maximum number of multicast groups that can be joined on a port" on page 165	Optional
"Configuring IGMP Snooping querier" on page 165	Optional

Enabling IGMP Snooping

Follow these steps to enable IGMP Snooping:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable IGMP Snooping	**igmp-snooping enable**	Required Disabled by default.
Enter VLAN view	**vlan** *vlan-id*	-
Enable IGMP Snooping	**igmp-snooping enable**	Required Disabled by default.

Configuring IGMP-Snooping timers

Follow these steps to configure IGMP-Snooping timers:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Configure an aging timer of router port	**igmp-snooping router-aging-time** *seconds*	Optional By default, the router port aging time is 105 seconds.
Configure a response-to-query timer	**igmp-snooping max-response-time** *seconds*	Optional By default, the maximum response-to-query time is 10 seconds.
Configure an aging timer of a member port of a multicast group	**igmp-snooping host-aging-time** *seconds*	Optional By default, the aging time of the multicast group member port is 260 seconds.

Configuring fast leave processing

1 Configure fast leave processing in system view

Follow these steps to configure fast leave processing in system view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Configure fast leave processing	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required Disabled by default

2 Configure fast leave in Ethernet port view

Follow these steps to configure fast leave processing in Ethernet port view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure fast leave processing	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required Disabled by default

Configuring a multicast group filter

1 Configure a multicast group filter in system view

Follow these steps to configure a multicast group filter in system view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required Disabled by default

2 Configure a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required Disabled by default

Configuring the maximum number of multicast groups that can be joined on a port

Follow these steps to configure the maximum number of multicast groups that can be joined on a port:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure maximum number of multicast groups that can be joined on the port	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**]]	Required The system default is 255.

Configuring IGMP Snooping querier

Follow these steps to configure IGMP Snooping querier:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable IGMP Snooping	**igmp-snooping enable**	Required Disabled by default
Enter VLAN view	**vlan** *vlan-id*	-
Enable IGMP Snooping	**igmp-snooping enable**	Required Disabled by default
Enable IGMP-Snooping querier	**igmp-snooping querier**	Required Disabled by default
Configure the query interval	**igmp-snooping query-interval** *seconds*	Optional The system default is 60 seconds.
Configure a source IP address for general query messages	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	Optional The system default is 0.0.0.0.

Configuring IGMP

Complete these tasks to configure IGMP:

Configuration task	Remarks
"Enabling IGMP" on page 166	Required
"Configuring IGMP version" on page 166	Optional
"Configuring parameters related to IGMP queries" on page 166	Optional
"Configuring the maximum allowed number of multicast groups" on page 167	Optional

Configuration task	Remarks
"Configuring a multicast group filter" on page 167	Optional
"Configuring simulated joining" on page 168	Optional
"Configuring IGMP proxy" on page 168	Optional
"Removing joined IGMP groups from an interface" on page 169	Optional

Enabling IGMP

Follow these steps to enable IGMP:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable multicast routing	**multicast routing-enable**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enabling IGMP	**igmp enable**	Required Disabled by default

CAUTION: *The following configurations in this chapter are implemented after multicast routing is enabled on the device and IGMP is enabled on the corresponding interface.*

Configuring IGMP version

Follow these steps to configure IGMP version:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Configure IGMP version	**igmp version** { **1** | **2** }	Required IGMPv2 by default

CAUTION: *The device cannot switch from one IGMP version to another automatically. All switches on the same subnet must run the same version of IGMP.*

Configuring parameters related to IGMP queries

Follow these steps to configure parameters related to IGMP queries:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Configure IGMP query interval	**igmp timer query** *seconds*	Optional The system default is 60 seconds.
Configure the IGMP last member query interval	**igmp lastmember-queryinterval** *seconds*	Optional The system default is 1 second.

To...	Use the command...	Remarks
Configure the IGMP last member query count	**igmp robust-count** *robust-value*	Optional The system default is two.
Configure the IGMP other querier present interval	**igmp timer other-querier-present** *seconds*	Optional The system default is 120 seconds, twice the interval specified by the **igmp timer query** command.
Configure the maximum response time	**igmp max-response-time** *seconds*	Optional The system default is 10 seconds.

Configuring the maximum allowed number of multicast groups

Follow these steps to configure the maximum number of multicast groups allowed to be joined on an interface:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Configure the maximum number of multicast groups allowed on the interface	**igmp group-limit** *limit*	Required The system default is 256.

CAUTION: *If you configure the maximum number of multicast groups allowed on an interface to 1, a new group joined on the interface automatically supersedes the existing one.*

If the number of existing multicast groups is larger than the limit configured on the interface, the system will remove the oldest entries automatically until the number of multicast groups on the interface conforms to the configured limit.

Configuring a multicast group filter

1 Configure a multicast group filter in VLAN interface view

Follow these steps to configure a multicast group filter in VLAN interface view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Configure a multicast group filter	**igmp group-policy** *acl-number* [**1** | **2** | **port** *interface-type interface-number* [**to** *interface-type interface-number*]]	Optional No filter is configured by default.

2 Configuring a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure a multicast group filter	**igmp group-policy** *acl-number* **vlan** *vlan-id*	Optional No multicast group filter is configured by default. The port must belong to the specified VLAN.

Configuring simulated joining

1 Configure simulated joining in VLAN interface view

Follow these steps to configure simulated joining in VLAN interface view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Configure simulated joining	**igmp host-join** *group-address* **port** *interface-list*	Optional Disabled by default

2 Configure simulated joining in Ethernet port view

Follow these steps to configure simulated joining in VLAN interface view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure simulated joining	**igmp host-join** *group-address* **vlan** *vlan-id*	Optional Disabled by default

CAUTION: *Before configuring simulated joining, you must enable IGMP in VLAN interface view.*

If you configure a port as a simulated host in Ethernet port view, the Ethernet port must belong to the specified VLAN; otherwise the configuration does not take effect.

Configuring IGMP proxy

Follow these steps to configure IGMP proxy:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable multicast routing	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable IGMP	**igmp enable**	Required

To...	Use the command...	Remarks
Configure IGMP proxy	**igmp proxy Vlan-interface** *interface-number*	Required Disabled by default

CAUTION:

- *You must enable PIM 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.*
- *When you configure the IP address of the interface that will serve as an IGMP proxy, make sure that the IP address is not the lowest on this subnet to prevent this interface from being elected as the IGMP querier on the subnet, as this will result in failure of multicast data forwarding.*

Removing joined IGMP groups from an interface

Follow these steps to remove joined IGMP groups from an interface:

To...	Use the command...	Remarks
Remove the specified group or all groups from the specified interface or all interfaces	**reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }	The **reset** command available in user view.

***CAUTION:** After a multicast group is removed from an interface, hosts attached to interface can join the multicast group again.*

Configuring PIM

Configuring PIM-DM

Follow these steps to configure PIM-DM:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable multicast routing	**multicast routing-enable**	Required Disabled by default
Enter PIM view	**pim**	-
Configure a multicast source or multicast source-group filter	**source-policy** *acl-number*	Optional You can define the related IP addresses in an ACL.
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-DM	**pim dm**	Required
Configure the hello interval on the interface	**pim timer hello** *seconds*	Optional The system default is 30 seconds.
Configure a limit on the number of PIM neighbors on the interface	**pim neighbor-limit** *limit*	Optional The default value is 128.

To...	Use the command...	Remarks
Configure the filtering policy for PIM neighbors	**pim neighbor-policy** *acl-number*	Optional You can define the related IP addresses in an ACL. Disabled by default

Configuring PIM-SM

Follow these steps to configure PIM-SM:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable multicast routing	**multicast routing-enable**	Required Disabled by default
Enter PIM view	**pim**	-
Configure a multicast source or multicast source-group filter	**source-policy** *acl-number*	Optional You can define the related IP addresses in an ACL.
Configure a C-BSR	**c-bsr** *interface-type interface-number hash-mask-len* [*priority*]	Optional By default, no C-BSR is configured. The default priority is 0.
Configure a C-RP	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority*]*	Optional By default, no C-RP is configured. The default priority is 0.
Configure a static RP	**static-rp** *rp-address* [*acl-number*]	Optional No static RP is configured by default.
Configure a legal BSR address range	**bsr-policy** *acl-number*	Optional No legal BSR address range is configured by default.
Configure a legal C-RP address range	**crp-policy** *acl-number*	Optional You can define the related IP address ranges in an ACL. No legal C-RP address range is configured by default.
Configure to filter the register messages from RP to DR	**register-policy** *acl-number*	Optional You can define the related IP addresses in an ACL. Disabled by default.
Disable RPT-to-SPT switchover	**spt-switch-threshold infinity** [**group-policy** *acl-number* [**order** *order-value*]]	Optional By default, the device switches to the SPT immediately after it receives the first multicast packet from the RPT.
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-SM	**pim sm**	Required

To...	Use the command...	Remarks
Configuring a PIM-SM domain boundary	**pim bsr-boundary**	Optional By default, no PIM-SM domain boundary is configured
Configure the hello interval on the interface	**pim timer hello** *seconds*	Optional The system default is 30 seconds.
Configure the maximum number of PIM neighbors allowed on the interface	**pim neighbor-limit** *limit*	Optional The default value is 128.
Configure the filtering policy for PIM neighbors	**pim neighbor-policy** *acl-number*	Optional You can define the related IP addresses in an ACL. Disabled by default

Configuring MSDP

Configuring MSDP basic functions

Follow these steps to configure MSDP basic functions:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enable MSDP and enter MSDP view	**msdp**	Required
Create an MSDP peer connection	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required You need to configure related parameters on both devices between which the peer connection is to be created. The peer ID is an address pair (the IP address of the local interface and the IP address of the remote MSDP peer).
Configure a static RPF peer	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	Optional For an area with only one MSDP peer, if BGP or MBGP is not running, you need to configure a static RPF peer.

Configuring MSDP peer connections

Complete these tasks to configure connection between MSDP peers:

Configuration task	Remarks
"Configure description information for MSDP peers" on page 171	Required
"Configure an MSDP mesh group" on page 172	Optional
"Configure MSDP peer connection control" on page 172	Optional

1 Configure description information for MSDP peers

Follow these steps to configure description information of an MSDP peer:

To...	Use the command...	Remarks
Enter system view	**system-view**	-

To...	Use the command...	Remarks
Enter MSDP view	**msdp**	-
Configure description information for an MSDP peer	**peer** *peer-address* **description** *text*	Optional No description information is configured for MSDP peers by default.

2 Configure an MSDP mesh group

Follow these steps to configure an MSDP mesh group:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Add an MSDP peer in a mesh group	**peer** *peer-address* **mesh-group** *name*	Required An MSDP peer does not belong to any mesh group by default.

- *Before grouping multiple routers into an MSDP mesh group, make sure that these routers are interconnected with one another.*
- *To add different MSDP peers into an MSDP mesh group, configure the same mesh group name on them.*
- *An MSDP peer can belong to only one mesh group. A newly configured mesh group name supersedes the existing one.*

3 Configure MSDP peer connection control

Follow these steps to configure MSDP peer connection control:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Shut down an MSDP peer	**shutdown** *peer-address*	Optional By default, MSDP peers are connected.
Configure the MSDP peer connection retry period	**timer retry** *seconds*	Optional The system default is 30 seconds.

Configuring SA message delivery

Complete these tasks to configure SA message delivery:

Configuration task	Remarks
"Configure the RP address in SA messages" on page 173	Optional
"Configure the SA message cache" on page 173	Optional
"Configure SA message transmission and filtering" on page 173	Optional
"Configure a rule for filtering multicast sources in SA messages" on page 174	Optional
"Configure a filtering rule for receiving or forwarding SA messages" on page 174	Optional

1 Configure the RP address in SA messages

Follow these steps to configure the RP address in SA messages:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Configure the RP address in SA messages	**originating-rp** *interface-type interface-number*	Optional By default, the RP address in an SA message is the PIM RP address.

In Anycast RP application, C-BSR and C-RP must be configured on different devices or ports.

2 Configure the SA message cache

Follow these steps to configure the SA message cache:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Enable the SA message cache mechanism	**cache-sa-enable**	Optional Enabled by default
Configure the maximum number of SA messages the router can cache	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	Optional The system default is 2048.

3 Configure SA message transmission and filtering

Follow these steps to configure SA message transmission and filtering:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Enable the SA message cache mechanism	**cache-sa-enable**	Optional After receiving an SA message, a router caches SA state by default.

To...	Use the command...	Remarks
Enable the router to send SA requests to the designated MSDP peer	**peer** *peer-address* **request-sa-enable**	Optional By default, upon receiving a new Join message, a router does not send an SA request message to its designated MSDP peer; instead it waits for the next SA message.
Configure a filtering rule for SA requests from the specified MSDP peer	**peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]	Optional Be default, a router receives all SA request messages from its MSDP peer.

4 Configure a rule for filtering multicast sources in SA messages

Follow these steps to configure a rule for filtering the multicast sources of SA messages:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Configure multicast source filtering at SA message creation	**import-source** [**acl** *acl-number*]	Optional By default, SA messages advertise all the (S, G) entries in the domain.

5 Configure a filtering rule for receiving or forwarding SA messages

Follow these steps to configure a filtering rule for receiving or forwarding SA messages:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Configure a filtering rule for receiving or forwarding SA messages	**peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]	Optional By default, no filtering rule is configured for receiving or forwarding SA messages, namely, all SA messages from MSDP peers will be accepted or forwarded.
Configure the minimum TTL required for an SA-encapsulated multicast packet to be forwarded to the specified MSDP peer	**peer** *peer-address* **minimum-ttl** *ttl-value*	Optional The system default is 0.

PIM-DM plus IGMP plus IGMP Snooping Configuration Example

Requirement Analysis

When users receive voice on demand (VOD) information through multicast, the information receiving mode may vary based on user requirements:

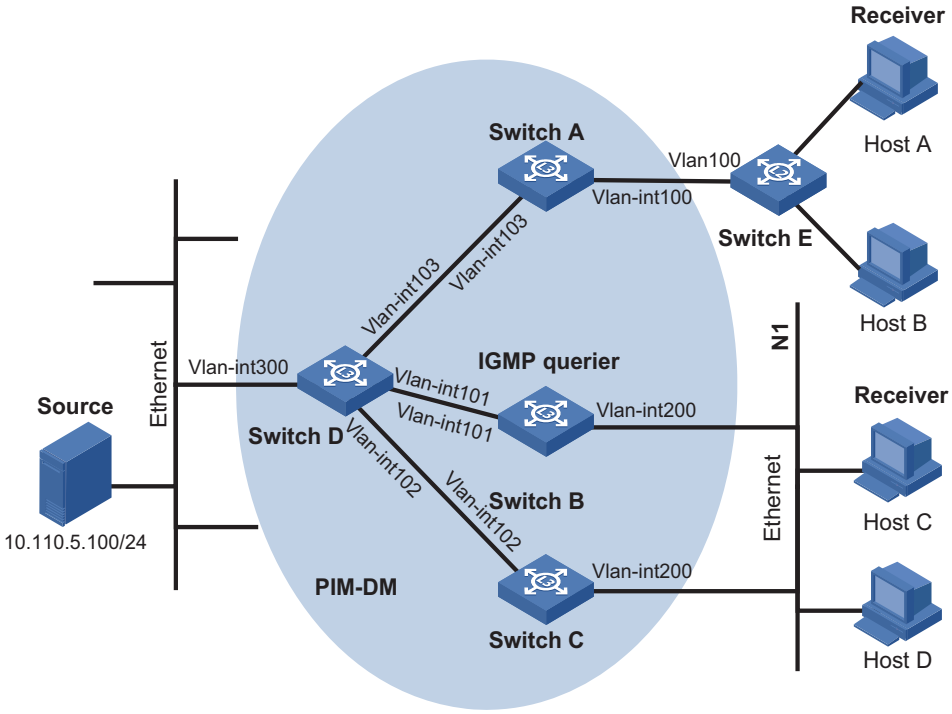
1. To avoid video broadcast at Layer 2, IGMP Snooping is enabled on Switch E, through which Host A and Host B receive the multicast data.
2. To ensure reliable and stable reception of multicast data, Switch B and Switch C provide uplink backup for the directly attached stub network N1, which comprises multicast receivers Host C and Host D.
3. All the Layer 3 switches run RIP for unicast routing and run PIM-DM for multicast routing.

Configuration Plan

1. Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
2. Switch A connects to Switch E through VLAN-interface 100, and to Switch D through VLAN-interface 103.
3. Switch B and Switch C connect to stub network N1 through their respective VLAN-interface 200, and to Switch D through VLAN-interface 101 and VLAN-interface 102 respectively.
4. Enable IGMPv2 on VLAN-interface 100 of Switch A. Enable IGMP Snooping on Switch E and in VLAN 100. Run IGMPv2 on Switch B, Switch C, and the hosts in stub network N1. Typically, Switch B acts as the IGMP querier.

Network Diagram

Figure 67 Network diagram for PIM-DM plus IGMP plus IGMP Snooping configuration



Device	Interface	IP address	Ports
Switch A	Vlan-int100	10.110.1.1/24	Ethernet1/0/1
	Vlan-int103	192.168.1.1/24	Ethernet1/0/2
Switch B	Vlan-int200	10.110.2.1/24	Ethernet1/0/1
	Vlan-int101	192.168.2.1/24	Ethernet1/0/2
Switch C	Vlan-int200	10.110.2.2/24	Ethernet1/0/1
	Vlan-int102	192.168.3.1/24	Ethernet1/0/2
Switch D	Vlan-int300	10.110.5.1/24	Ethernet1/0/1
	Vlan-int103	192.168.1.2/24	Ethernet1/0/2
	Vlan-int101	192.168.2.2/24	Ethernet1/0/3
	Vlan-int102	192.168.3.2/24	Ethernet1/0/4
Switch E	Vlan 100	-	Ethernet1/0/1, Ethernet1/0/2, Ethernet1/0/3

Configuration Procedure

Configuring VLANs, VLAN interfaces and IP addresses on each switch

Configure VLANs, VLAN interfaces, and their IP addresses on Switch A.

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 103
[SwitchA-vlan103] port Ethernet 1/0/2
[SwitchA-vlan103] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.110.1.1 24
```

```
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 103
[SwitchA-Vlan-interface103] ip address 192.168.1.1 24
[SwitchA-Vlan-interface103] quit
```

Configure VLANs, VLAN interfaces, and their IP addresses on other switches as per Figure 67. The detailed configuration steps are omitted here.

Configuring the unicast routing protocol

Enable RIP on Switch A, and then enable RIP on subnets 192.168.1.0 and 10.110.1.0.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA- rip] network 192.168.1.0
[SwitchA- rip] network 10.110.1.0
[SwitchA- rip] quit
```

The configuration on Switch B, Switch C, and Switch D is similar to the configuration on Switch A.

Configuring the multicast protocols

Enable IP multicast routing on Switch A, enable PIM-DM on each interface, and then enable IGMPv2 on VLAN-interface 100.

```
<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 multicast routing on Switch D, and enable PIM-DM on each interface.

```
<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
```

Enable IGMP Snooping on Switch E, and enable IGMP Snooping in VLAN 100.

```
<SwitchE> system-view
[SwitchE] igmp-snooping enable
  Enable IGMP-Snooping ok.
[SwitchE] vlan 100
[SwitchE-vlan100] igmp-snooping enable
[SwitchE-vlan100] quit
```

Verifying the configuration

Now start sending multicast data to multicast group 224.1.1.1 from Source and start receiving the multicast data on Host A, and take the following steps to verify the configurations made on the switches.

1 Check whether the multicast stream can flow to Host A.

View the PIM neighboring relationships on Switch D.

```
<SwitchD> display pim neighbor
Neighbor's Address  Interface Name                Uptime    Expires
192.168.2.1         Vlan-interface101             02:45:04  00:04:46
192.168.3.1         Vlan-interface102             02:42:24  00:04:45
192.168.1.1         Vlan-interface103             02:43:44  00:05:44
```

View the multicast forwarding table of Switch D.

```
<SwitchD>display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entries: 0 entry created by IP, 1 entries created by protocol

00001. (10.110.5.110, 224.1.1.1), iif Vlan-interface1, 1 oifs,
     Protocol Create
     List of outgoing interface:
       01: Vlan-interface101
     Matched 181 pkts(271500 bytes), Wrong If 0 pkts
     Forwarded 130 pkts(195000 bytes)

Total 1 entries Listed
```

View the multicast forwarding table of Switch A.

```
<SwitchA>display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.110.5.110, 224.1.1.1), iif Vlan-interface101, 1 oifs,
     Protocol Create
     List of outgoing interface:
       01: Vlan-interface100
     Matched 451 pkts(676500 bytes), Wrong If 0 pkts
     Forwarded 451 pkts(676500 bytes)

Total 1 entry Listed
Matched 1 entry
```

View the multicast group information that contains port information on Switch A.

```
<SwitchA> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).
```

```
  Vlan(id):101.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/2
  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/15
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/15
```

View the information about the multicast group entries created by IGMP Snooping on Switch E.

```
<SwitchE> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/2
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/19
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/19
```

The above-mentioned information shows that multicast forwarding entries have been correctly established on Switch D and Switch A, and multicast traffic can successfully flow to Host A.

2 Configure IGMP Snooping multicast group filtering on Switch E

Configure to filter the packets for the multicast group 224.1.1.1 on Switch E.

```
<SwitchE> system-view
[SwitchE-acl-basic-2000] rule deny source 224.1.1.1 0
[SwitchE-acl-basic-2000] rule permit source any
[SwitchE-acl-basic-2000] quit
[SwitchE]igmp-snooping group-policy 2000 vlan 100
```

View multicast forwarding entries on Switch A.

```
<SwitchA> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.110.5.100, 224.1.1.1), iif Vlan-interface101, 0 oifs,
     Protocol Create
     Matched 5 pkts(7500 bytes), Wrong If 0 pkts
```

```
     Forwarded 0 pkts(0 bytes)

Total 1 entry Listed
```

As shown above, Switch A has stopped forwarding multicast data for the multicast group 224.1.1.1.

View multicast group information on Switch E.

```
<SwitchE> display igmp-snooping group
  Total 0 IP Group(s).
  Total 0 MAC Group(s).

  Vlan(id):200.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/19
```

With multicast group filtering enabled, the corresponding ports drop IGMP reports for the filtered group and will be removed for that group when their respective port aging timer expires.

3 Configure IGMP multicast group filtering on Switch A.

Disable multicast group filtering on Switch E.

```
<SwitchE> system-view
[SwitchE] undo igmp-snooping group-policy
```

To verify the configuration of IGMP multicast group filtering on Switch A, disable IGMP Snooping multicast group filtering on Switch E first.

Configure to filter the multicast group 224.1.1.1 on VLAN-interface 100 of Switch A, and then display the multicast forwarding entries of Switch A.

Configure to filter the multicast group 224.1.1.1 on VLAN-interface 100 of Switch A.

```
<SwitchA> system-view
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule deny source  224.1.1.1 0
[SwitchA-acl-basic-2000] rule permit source any
[SwitchA-acl-basic-2000] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] igmp group-policy 2000
[SwitchA-Vlan-interface100] return
```

View multicast forwarding entries on Switch A.

```
<SwitchA> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.110.5.100, 224.1.1.1), iif Vlan-interface101, 0 oifs,
     Protocol Create
     Matched 5 pkts(7500 bytes), Wrong If 0 pkts
     Forwarded 0 pkts(0 bytes)
```

```
Total 1 entry Listed
```

View multicast group information on Switch A.

```
<SwitchA> display igmp group
 Total 0 IGMP groups reported on this router
```

After multicast group filtering is enabled, the corresponding port cannot receive IGMP reports. Thus, the corresponding multicast groups are deleted after the port aging timer expires.

As shown above, IGMP Snooping multicast group filtering has the same function as IGMP multicast group filtering. You can use either approach based on the specific situation.

PIM-SM plus IGMP plus IGMP Snooping Configuration Examples

Requirement Analysis

When users receive VOD information through multicast, the information receiving mode may vary based on user requirements:

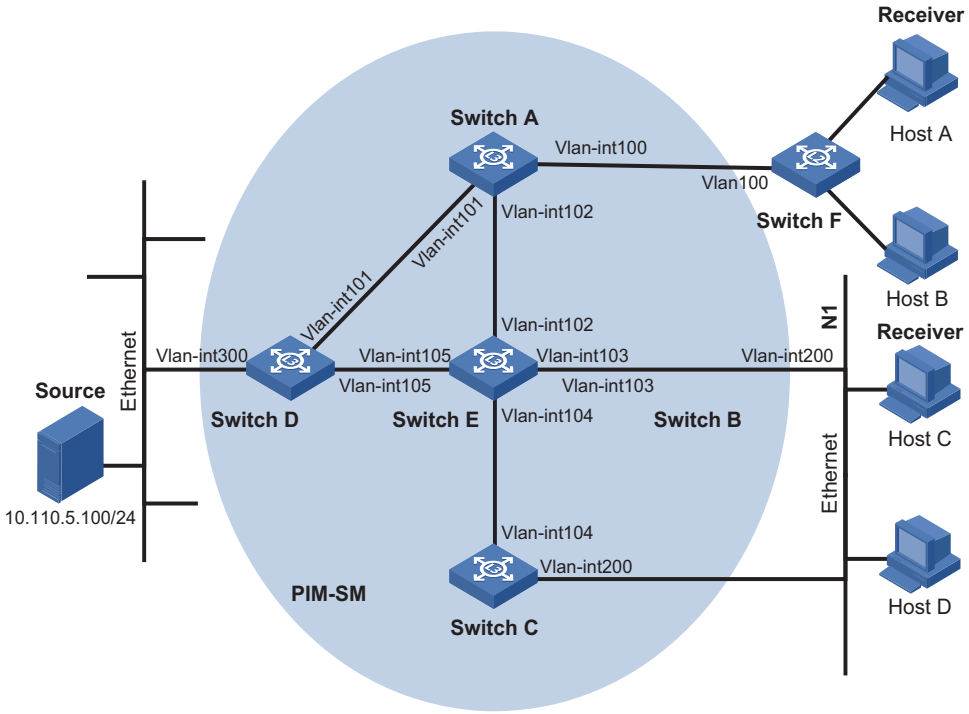
1. To avoid broadcasting of the video information at Layer 2, IGMP Snooping is enabled on Switch E, through which Host A and Host B receive the multicast data.
2. To ensure reliable and stable reception of multicast data, Switch B and Switch C provide uplink backup for the directly attached stub network N1, which comprises multicast receivers Host C and Host D.
3. Configure the PIM-SM domain as a single-BSR domain. Run OSPF for unicast routing in the domain.

Configuration Plan

1. Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
2. Switch A connects to Switch F through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
3. Switch B and Switch C connect to stub network N1 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
4. It is required that VLAN-interface 105 of Switch D and VLAN-interface 102 of Switch E act as C-BSR and C-RP.
5. IGMPv2 is required on VLAN-interface 100 of Switch A. IGMP Snooping is required on Switch F and in VLAN 100. IGMPv2 is also required between Switch B, Switch C, and stub network N1. Typically, Switch B acts as the querier.

Network Diagram

Figure 68 Network diagram for PIM-SM plus IGMP plus IGMP Snooping configuration



Device	Interface	IP address	Ports
Switch A	Vlan-int100	10.110.1.1/24	Ethernet1/0/1
	Vlan-int101	192.168.1.1/24	Ethernet1/0/2
	Vlan-int102	192.168.9.1/24	Ethernet1/0/3
Switch B	Vlan-int200	10.110.2.1/24	Ethernet1/0/1
	Vlan-int103	192.168.2.1/24	Ethernet1/0/2
Switch C	Vlan-int200	10.110.2.2/24	Ethernet1/0/1
	Vlan-int104	192.168.3.1/24	Ethernet1/0/2
Switch D	Vlanint300	10.110.5.1/24	Ethernet1/0/1
	Vlanint101	192.168.1.2/24	Ethernet1/0/2
	Vlanint105	192.168.4.2/24	Ethernet1/0/3
Switch E	Vlanint104	192.168.3.2/24	Ethernet1/0/3
	Vlanint103	192.168.2.2/24	Ethernet1/0/2
	Vlanint102	192.168.9.2/24	Ethernet1/0/1
	Vlanint105	192.168.4.1/24	Ethernet1/0/4
Switch F	Vlan 100	-	Ethernet1/0/1, Ethernet1/0/2, Ethernet1/0/3

Configuration Procedure

Configuring VLANs, VLAN interfaces and IP addresses for each switch

Configure VLANs, VLAN interfaces, and their IP addresses on Switch A.

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1
[SwitchA-vlan100] quit
```

```
[SwitchA] vlan 101
[SwitchA-vlan101] port Ethernet 1/0/2
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port Ethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.110.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 101
[SwitchA-Vlan-interface101] ip address 192.168.1.1 24
[SwitchA-Vlan-interface101] quit
[SwitchA] interface Vlan-interface 102
[SwitchA-Vlan-interface102] ip address 192.168.9.1 24
[SwitchA-Vlan-interface102] quit
```

Configure VLANs, VLAN interfaces, and their IP addresses on other switches as per Figure 68. The detailed configuration steps are omitted here.

Configuring the unicast routing protocol

Configure a router ID and enable OSPF on Switch A.

```
<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 10.110.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0]network 192.168.9.0 0.0.0.255
```

The configuration on Switch B, Switch C, Switch D, and Switch E is similar to the configuration on Switch A.

Configuring the multicast protocols

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and then enable IGMPv2 on VLAN-interface 100.

```
<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
```

It is necessary to enable IGMP only on interfaces with attached multicast receivers. As the default IGMP version is IGMPv2, it is not necessary to use the version configuration command on the interface.

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.

Configure the group range to be served by the RP and configure a C-BSR and a C-RP on Switch D.

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 105 24 2
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005 priority 2
[SwitchD-pim] quit
```

Configure the group range to be served by the RP and configure a C-BSR and a 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 24 1
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005 priority 1
[SwitchE-pim] quit
```

Enable IGMP Snooping globally on Switch E, and enable IGMP Snooping in VLAN 100.

```
<SwitchF> system-view
[SwitchF] igmp-snooping enable
  Enable IGMP-Snooping ok.
[SwitchF] vlan 100
[SwitchF-vlan100] igmp-snooping enable
[SwitchF-vlan100] quit
```

Verifying the configuration

Now start sending multicast data to multicast group 225.1.1.1 from Source and start receiving the multicast data on Host A and Host C, and take the following steps to verify the configurations made on the switches.

1 Check whether the multicast stream flows to Host A and Host C.

View 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
```

View BSR information on Switch E.

```
<SwitchE> display pim bsr-info
  Current BSR Address: 192.168.4.2
              Priority: 2
           Mask Length: 24
               Expires: 00:01:39
  Local Host is C-BSR: 192.168.9.2
```

```
            Priority: 1
          Mask Length: 24
```

View RP information on Switch E.

```
<SwitchE> display pim rp-info
 PIM-SM RP-SET information:
    BSR is: 192.168.4.2

    Group/MaskLen: 225.1.1.0/24
      RP 192.168.9.2
        Version: 2
        Priority: 1
        Uptime: 00:03:15
        Expires: 00:01:14
      RP 192.168.4.2
        Version: 2
        Priority: 2
        Uptime: 00:04:25
        Expires: 00:01:09
```

View PIM routing table entries on Switch A.

```
<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 information on Switch B and Switch C is similar to that on Switch A.

View PIM routing table entries on Switch D.

```
<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
```

View PIM routing table entries on Switch E.

```
<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
    Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
    Uptime: 00:02:34, Timeout in 176 sec
    Upstream interface: Null, RPF neighbor: 0.0.0.0
    Downstream interface list:
      Vlan-interface102, Protocol 0x100: RPT, timeout in 176 sec
      Vlan-interface103, Protocol 0x100: SPT, timeout in 135 sec

(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-interface105, RPF neighbor: 192.168.4.2
    Downstream interface list:
      Vlan-interface102, Protocol 0x200: SPT, timeout in 147 sec
      Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec
Matched 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry
```

View the information about multicast group entries created by IGMP Snooping on Switch F.

```
<SwitchF> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/2
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/19
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/19
```

View multicast group information that contains port information on Switch B.

```
<SwitchB> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/24
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/24
```

```
  Vlan(id):103.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/10
```

As shown above, multicast traffic can successfully flow to Host A and Host C.

2 Configure simulated joining

Configure simulated joining on Switch B, thus to prevent the multicast switch from considering that no multicast receiver exist on the subnet due to some reason and removing the corresponding path from the multicast forwarding tree.

Configure Ethernet 1/0/21 as a simulated host to join multicast group 225.1.1.1.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 200
[SwitchB-Vlan-interface200] igmp host-join 225.1.1.1 port Ethernet 1/0/21
```

View multicast group information that contains port information on Switch B.

```
<SwitchB> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/21             Ethernet1/0/24
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/21             Ethernet1/0/24

  Vlan(id):103.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/10
```

As shown above, Ethernet 1/0/21 has become a member port for multicast group 225.1.1.1.

IGMP Snooping-Only Configuration Examples

Network Requirements

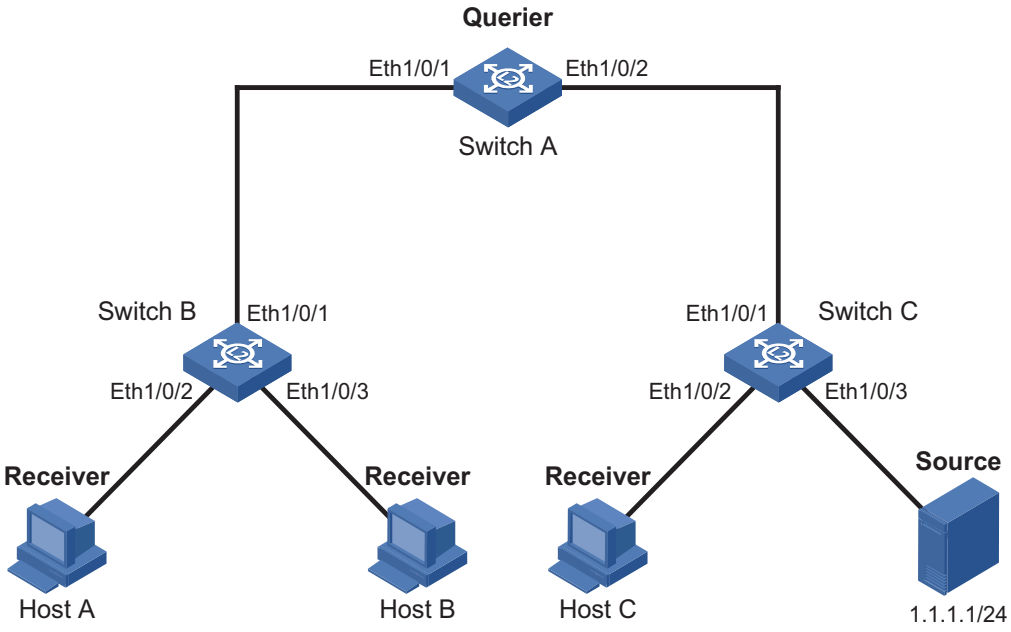
In case that it is unnecessary or infeasible to build a Layer-3 multicast network, enabling IGMP Snooping on all the devices in a Layer 2 network can implement some multicast functions.

Configuration Plan

1. As shown in Figure 69, in a Layer-2 network without Layer-3 devices, Switch C connects to the multicast source through Ethernet 1/0/3. At least one receiver is attached to Switch B and Switch C respectively.
2. Enable IGMP Snooping on Switch A, Switch B, and Switch C, with Switch A acting as the IGMP Snooping querier.
3. Enable Switch A and Switch B to drop unknown multicast traffic so that multicast traffic for unknown multicast groups are not flooded in the VLAN.

Network Diagram

Figure 69 Network diagram for IGMP Snooping-only configuration



Configuration Procedure

Configuring switch A

Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
Enable IGMP-Snooping ok.
```

Create VLAN 100, add Ethernet 1/0/1 and Ethernet 1/0/2 into VLAN 100, and then enable IGMP Snooping in this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 Ethernet 1/0/2
[SwitchA-vlan100] igmp-snooping enable
```

Enable IGMP Snooping querier in VLAN 100.

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

Enable the function of dropping unknown multicast packets.

```
[SwitchA] unknown-multicast drop enable
```

Configuring Switch B

Enable IGMP Snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
Enable IGMP-Snooping ok.
```

Create VLAN 100, add Ethernet 1/0/1 through Ethernet 1/0/3 into VLAN 100, and then enable IGMP Snooping in this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/3
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Enable the function of dropping unknown multicast packets.

```
[SwitchB] unknown-multicast drop enable
```

Configuring Switch C

Enable IGMP Snooping globally.

```
<SwitchC system-view
[SwitchC] igmp-snooping enable
Enable IGMP-Snooping ok.
```

Create VLAN 100, add Ethernet 1/0/1 through Ethernet 1/0/3 into VLAN 100, and then enable IGMP Snooping in this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/3
[SwitchC-vlan100] igmp-snooping enable
```

CAUTION: *Switch C is not the IGMP Snooping querier, so it does not have member ports for non-directly-connected hosts, and the corresponding forwarding entries cannot be created on it. Therefore, do not enable the function of dropping unknown multicast packets on Switch C. To avoid impact on the network and on Switch C caused by multicast flooding, it is recommended to enable IGMP Snooping querier on the switch to which the multicast source is directly attached.*

Verifying the configuration

1 View information on Switch B.

View IGMP packet statistics on Switch B.

```
<SwitchB> display igmp-snooping statistics
  Received IGMP general query packet(s) number:16.
  Received IGMP specific query packet(s) number:3.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:53.
  Received IGMP leave packet(s) number:1.
  Received error IGMP packet(s) number:0.
  Sent IGMP specific query packet(s) number:1.
```

Switch B received IGMP general queries sent by the querier and IGMP reports from receivers.

View multicast group information on Switch B.

```
<Switch B> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/1
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/2
    MAC group(s):
        MAC group address:0100-5e7f-fffe
        Host port(s):Ethernet1/0/2
```

As shown above, a forwarding entry for the multicast group 224.1.1.1 has been created on Switch A, with Ethernet 1/0/1 as the router port and Ethernet 1/0/2 as the member port.

2 View information on Switch A.

View IGMP packet statistics on Switch A.

```
<SwitchA> display igmp-snooping statistics
  Received IGMP general query packet(s) number:0.
  Received IGMP specific query packet(s) number:0.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:53.
  Received IGMP leave packet(s) number:1.
  Received error IGMP packet(s) number:0.
  Sent IGMP specific query packet(s) number:1.
```

Switch A receives IGMP reports from the receivers.

View multicast group information on Switch A.

```
<Switch A> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/1
    MAC group(s):
        MAC group address:0100-5e7f-fffe
        Host port(s):Ethernet1/0/1
```

As shown above, a forwarding entry for the multicast group 224.1.1.1 has been created on Switch A, with Ethernet 1/0/1 as the member port. Acting as the IGMP Snooping querier, Switch A does not have a router port.

3 View information on Switch C.

View IGMP packet statistics on Switch C.

```
<SwitchC> display igmp-snooping statistics
  Received IGMP general query packet(s) number:10.
  Received IGMP specific query packet(s) number:0.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:0.
  Received IGMP leave packet(s) number:.0
  Received error IGMP packet(s) number:0.
  Sent IGMP specific query packet(s) number:0.
```

Switch C received only IGMP general queries from the querier.

View multicast group information on Switch C.

```
<Switch C> display igmp-snooping group
  Total 0 IP Group(s).
  Total 0 MAC Group(s).

Vlan(id):100.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/1
```

As shown above, no forwarding entries have been created on Switch C. The switch must flood multicast data in the VLAN to allow the multicast data to flow to the receivers downstream; therefore, do not enable the function of dropping unknown multicast packets on Switch C.

MSDP Configuration Examples

Network Requirements

To enable communication between receivers and multicast sources in different PIM-SM domains, use MSDP to establish MSDP peering relationships between the RPs of different PIM-SM domains, so that these RPs can forward SA messages between PIM-SM domains to share multicast source information.

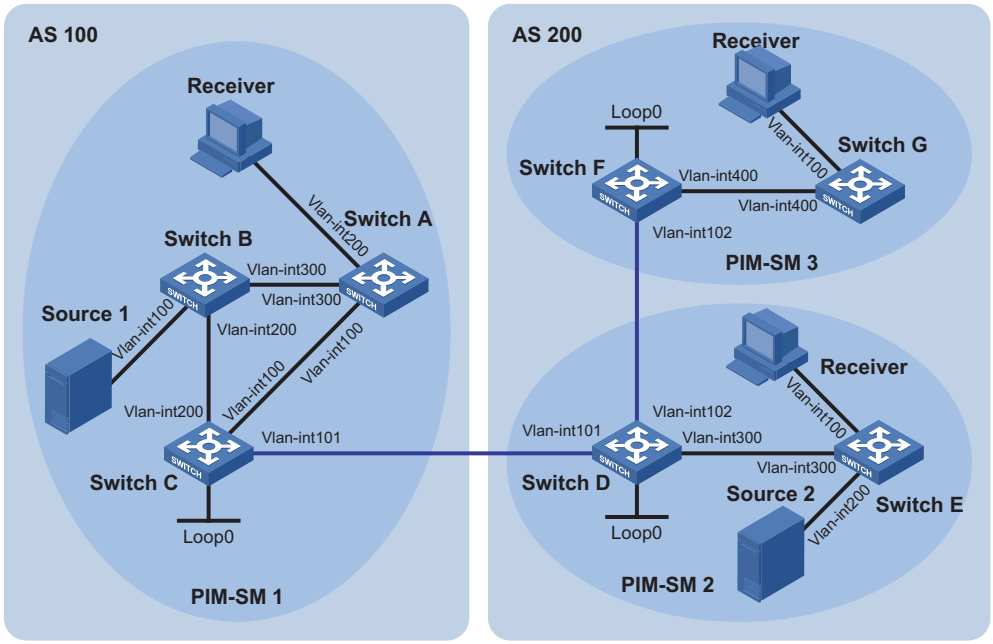
Configuration Plan

- Two ISPs maintain their respective ASs, AS 100 and AS 200. OSPF runs within each AS, and BGP is deployed for interoperability between the two ASs.
- PIM-SM 1 belongs to AS 100. PIM-SM 2 and PIM-SM 3 belong to AS 200.
- Both PIM-SM domains have 0 or 1 multicast source and at least one receiver. OSPF runs within each domain for unicast routing.
- The respective loopback interfaces, Loopback 0, of Switch C, Switch D and Switch F are configured as C-BSRs and C-RPs of the respective PIM-SM domains.

- Establish MSDP peering relationship between Switch C and Switch D through EBGP. Establish MSDP peering relationship between Switch D and Switch F through IBGP.

Network Diagram

Figure 70 Network diagram for MSDP configuration



Device	Interface	IP address	Device	Interface	IP address
SwitchA	Vlan-int100	10.110.1.2/24	Switch D	Vlan-int300	10.110.4.1/24
	Vlan-int200	10.110.6.1/24		Vlan-int102	192.168.3.1/24
	Vlan-int300	10.110.5.1/24		Vlan-int101	192.168.1.2/24
SwitchB	Vlan-int100	10.110.7.1/24		Loop0	2.2.2.2/32
	Vlan-int200	10.110.2.2/24	Switch E	Vlan-int100	10.110.8.1/24
	Vlan-int300	10.110.5.2/24		Vlan-int200	10.110.9.1/24
Switch C	Vlan-int100	10.110.1.1/24		Vlan-int300	10.110.4.2/24
	Vlan-int200	10.110.2.1/24		Loop0	2.2.2.2/32
	Vlan-int101	192.168.1.1/24	Switch F	Vlan-int400	10.110.3.1/24
	Loop0	1.1.1.1/32		Vlan-int102	192.168.3.2/24
				Loop0	3.3.3.3/32
			SwitchG	Vlan-int100	10.110.10.1/24
				Vlan-int400	10.110.3.2/24

Configuration Procedure

Configuring an interface IP address and a unicast routing protocol for each switch

Configure an IP address and a subnet mask for each interface as per Figure 70. The detailed configuration steps are not discussed in this document.

Configure OSPF for interoperation between switches in each PIM-SM domain. Ensure the network-layer interoperation among Switch A, Switch B and Switch C

in PIM-SM 1, the network-layer interoperation between Switch D and Switch E in PIM-SM 2, and the network-layer interoperation between Switch F and Switch G in PIM-SM 3, and ensure the dynamic update of routing information between the switches in each PIM-SM domain through the unicast routing protocol.

Configuring a unicast routing protocol for each AS

Configure OSPF on Switch C.

```
<SwitchC> system-view.
[SwitchC]ospf
[SwitchC-ospf-1]area 0
[SwitchC-ospf-1-area-0.0.0.0]network 10.110.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0]network 10.110.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
```

The configuration on Switch A, Switch B, Switch D, Switch E, Switch F and Switch G is similar to the configuration on Switch C.

Configuring a multicast routing protocol

1 Enable IP multicast routing, enable PIM-SM on each interface, and enable IGMP on the interfaces connected with receivers.

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and enable IGMP on VLAN-interface 200.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] igmp enable
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface101] pim sm
```

The configuration on Switch E and Switch G is similar to the configuration on Switch A. The specific configuration steps are omitted here.

Enable IP multicast routing on Switch C and enable PIM-SM on each interface.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim sm
```

The configuration on Switch B, Switch D, and Switch F is similar to the configuration on Switch C. The specific configuration steps are omitted here.

Configure a BSR boundary on Switch C.

```
[SwitchC-Vlan-interface101] pim bsr-boundary
[SwitchC-Vlan-interface101] quit
```

The configuration on Switch D and Switch F is similar to the configuration on Switch C.

2 Configure the position of interface Loopback 0, C-BSR, and C-RP.

Configure the position of Loopback 0, C-BSR, and C-RP on Switch C.

```
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] ip address 1.1.1.1 255.255.255.255
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 0 24
[SwitchC-pim] c-rp loopback 0
[SwitchC-pim] quit
```

The configuration on Switch D and Switch F is similar to the configuration on Switch C.

Configuring inter-AS BGP for mutual route redistribution between BGP and OSPF

Configure EBGP on Switch C, and configure OSPF route redistribution.

```
[SwitchC] bgp 100
[SwitchC-bgp] group 100 external
[SwitchC-bgp] peer 192.168.1.2 group 100 as-number 200
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] import-route direct
[SwitchC-bgp] quit
```

Configure IBGP and EBGP on Switch D, and configure OSPF route redistribution.

```
[SwitchD] bgp 200
[SwitchD-bgp] group 100 external
[SwitchD-bgp] group 200
[SwitchD-bgp] peer 192.168.1.1 group 100 as-number 100
[SwitchD-bgp] peer 192.168.3.2 group 200
[SwitchD-bgp] import-route ospf 1
[SwitchD-bgp] import-route direct
[SwitchD-bgp] quit
```

Configure IBGP on Switch F, and configure OSPF route redistribution.

```
[SwitchF] bgp 200
[SwitchF-bgp] group 200
[SwitchF-bgp] peer 192.168.3.1 group 200
[SwitchF-bgp] import-route ospf 1
[SwitchF-bgp] import-route direct
[SwitchF-bgp] quit
```

Configure BGP route redistribution to OSPF on Switch C.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route bgp
[SwitchC-ospf-1] quit
```

The configuration on Switch D and Switch F is similar to the configuration on Switch C.

Carry out the **display bgp peer** command to view the BGP peering relationships between the switches. For example:

View the information about BGP peering relationships on Switch C.

```
[SwitchC] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.1.2       200  4          0        950        945   15:41:14 Established
```

View the information about BGP peering relationships on Switch D.

```
[SwitchD] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.1.1       100  4          0        946        953   15:43:32 Established
192.168.3.2       200  4          0        946        954   15:41:18 Established
```

View the information about BGP peering relationships on Switch F.

```
[SwitchF] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.3.1       200  4          0        953        948   15:42:23 Established
```

Configuring MSDP peers

Configure an MSDP peer on Switch C.

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchC-msdp] quit
```

Configure an MSDP peer on Switch D.

```
[SwitchD] msdp
[SwitchD-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchD-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
[SwitchD-msdp] quit
```

Configure MSDP peers on Switch F.

```
[SwitchF] msdp
[SwitchF-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
[SwitchF-msdp] quit
```

When the multicast source Source 1 sends multicast information, receivers in PIM-SM2 and PIM-SM3 can receive the multicast data. You can use the **display msdp brief** command to view the brief information of MSDP peering relationships between the switches. For example:

View the brief information about MSDP peering relationships on Switch C.

```
[SwitchC] display msdp brief
MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.1.2         Up        00:12:27         200    13          0
```

View the brief information about MSDP peering relationships on Switch D.

```
[SwitchD] display msdp brief
MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.2         Up        00:15:32         200    8           0
 192.168.1.1         UP        00:06:39         100    13          0
```

View the brief information about MSDP peering relationships on Switch F.

```
[SwitchF] display msdp brief
MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.1         UP          01:07:08        200    8           0
```

View the detailed MSDP peer information on Switch C.

```
[SwitchC] display msdp peer-status
  MSDP Peer 192.168.1.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: Vlan-interface101 (192.168.1.1)
    Number of sent/received messages: 16/16
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:17:51
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
```

7 VLAN CONFIGURATION EXAMPLES

Keywords:

VLAN, 802.1q, VLAN interface, protocol VLAN

Abstract:

This document introduces how VLAN of the 3Com series Ethernet switches is applied and configured in practical networking implementations and how protocols are used in conjunction with VLANs.

Acronyms:

VLAN (Virtual local area network)

VLAN Support Matrix

Support for VLAN on 3Com Stackable Switches

Table 88 Support for VLAN on 3Com stackable switches

Feature (right) Model (below)	802.1Q VLAN	VLAN interface	Protocol VLAN
Switch 5500	●	●	●
Switch 4500	●	●	●
Switch 5500Gs	●	●	●
Switch 4200	●	❍	●
Switch 4210	●	❍	-
Switch 4210 52-Port	●	●	-
E352/E328	●	●	●
E126	●	❍	-
E152	●	❍	-

- *In the above table, the solid dots (●) indicate that the corresponding models provide full support for the function; the hollow dots (❍) indicate that the corresponding models provide incomplete support for the function, that is, the corresponding models support only the VLAN-interface for the management VLAN; the dashes (-) indicate that the corresponding models do not support the function.*
- *For detailed information about the support of your device for VLAN, refer to the user manual for your device.*

Configuration Guide

- *The configuration procedure differs by device. In this guide, the Switch 5500 is used as an example. For informaiton on how to configure VLAN on other models, refer to the Configuration Guide for that model.*
- *The configuration example in this guide provides only basic configuration procedures. For detailed information about individual functions, refer to the Configuraiton Guide and Command Reference Guide for that model.*

Configuring Basic VLAN Settings

The 3Com series switches support IEEE 802.1Q VLAN. The technology allows you to organize Ethernet ports into virtual workgroups by assigning them to different VLANs.

Follow these steps to create a VLAN and perform basic VLAN configuration:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Create multiple VLANs in bulk	**vlan** { *vlan-id1* **to** *vlan-id2* | **all** }	Optional
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required By default, only one default VLAN (VLAN 1) exists in the system.
Assign a name for the current VLAN	**name** *text*	Optional By default, the name of a VLAN is its VLAN ID, for example, **VLAN 0001**.
Configure the description of the current VLAN	**description** *text*	Optional By default, the description of a VLAN is its VLAN ID, for example, **VLAN 0001**.
Display VLAN information	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **dynamic** | **static**]	Available in any view

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

Follow these steps to assign a port to a VLAN in VLAN view:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	-
Assign a list of Ethernet ports to the VLAN	**port** *interface-list*	Required By default, all ports belong to the default VLAN (VLAN 1).

Only access ports can be assigned to a VLAN in VLAN view. You can assign trunk or hybrid ports to a VLAN only in Ethernet port view.

Follow these steps to assign a port to a VLAN in Ethernet port view:

To...		Use the command...	Remarks
Enter system view		**system-view**	-
Enter Ethernet port view		**interface** *interface-type interface-number*	-
Configure the port type		**port link-type** { **access** | **trunk** | **hybrid** }	Optional By defaults, all ports are access ports.
Assign the current port to the specified VLAN(s)	For an access port	**port access vlan** *vlan-id*	Required By default, all the three types of ports belong to the default VLAN (VLAN 1).
	For a trunk port	**port trunk permit vlan** { *vlan-id-list* | **all** }	
	For a hybrid port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	
Specify the default VLAN for the current port	For a trunk port	**port trunk pvid vlan** *vlan-id*	Optional By default, the default VLAN of an Ethernet port is VLAN 1. Because an access port can be assigned to only one VLAN, its default VLAN is the VLAN to which it belongs. Therefore, you do not need to configure a default VLAN for it.
	For a hybrid port	**port hybrid pvid vlan** *vlan-id*	

Configuring Basic Settings of a VLAN Interface

You can enable your switch to perform Layer 3 forwarding by configuring VLAN interfaces with IP addresses on the switch.

Follow these steps to configure basic settings of a VLAN interface:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Create a VLAN interface and enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required By default, no VLAN interface exists.
Assign an IP address to the current VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	Required No IP address is assigned to any VLAN interface by default.
Configure the description of the current VLAN interface	**description** *text*	Optional By default, the description of a VLAN interface is its name, for example, **Vlan-interface1 Interface**.

To...	Use the command...	Remarks
Shut down the VLAN interface	**shutdown**	Optional
Bring up the VLAN interface	**undo shutdown**	By default, a VLAN interface is in the up state. In this case, the VLAN interface is up so long as one port in the VLAN is up and goes down if all ports in the VLAN go down. An administratively shut down VLAN interface however will be in the down state until you bring it up, regardless of how the state of the ports in the VLAN changes.
Display information about the VLAN interface	**display interface Vlan-interface** [*vlan-id*]	Available in any view

- *Before creating a VLAN interface for a VLAN, create the VLAN first.*
- *On some 3Com series switches, only one VLAN interface is supported, and you must configure its VLAN as the default VLAN with the* ***management-vlan*** *command before creating the VLAN interface. For detailed configurations, refer to the corresponding user manual.*

Protocol VLAN Configuration

Protocol VLAN enables your switch to assign an incoming untagged frame to a VLAN based on its protocol. To configure a protocol VLAN, first create a protocol template to enable protocol VLAN, and then assign Ethernet ports to the protocol VLAN.

Follow these steps to configure a protocol VLAN:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	-
Create a protocol template	**protocol-vlan** [*protocol-index*] { **at** | **ip** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* **ssap** *ssap-id* } | **snap etype** *etype-id* } }	Required No protocol template exists by default.
Return to system view	**quit**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port as a hybrid port	**port link-type hybrid**	Required All Ethernet ports are access ports by default.
Assign the port to the protocol VLAN and configure the port to forward the frames of the VLAN with their VLAN tag removed	**port hybrid vlan** *vlan-id* **untagged**	Required All ports belong to VLAN 1 by default.

To...	Use the command...	Remarks
Associate the port with the protocol VLAN	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-index-end*] | **all** }	Required By default, an Ethernet port is not associated with any protocol VLAN.
Display information about the protocol templates of the specified VLAN(s)	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	Available in any view
Display information about the protocol templates of the protocol VLANs associated with the specified port(s)	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

VLAN Configuration Example

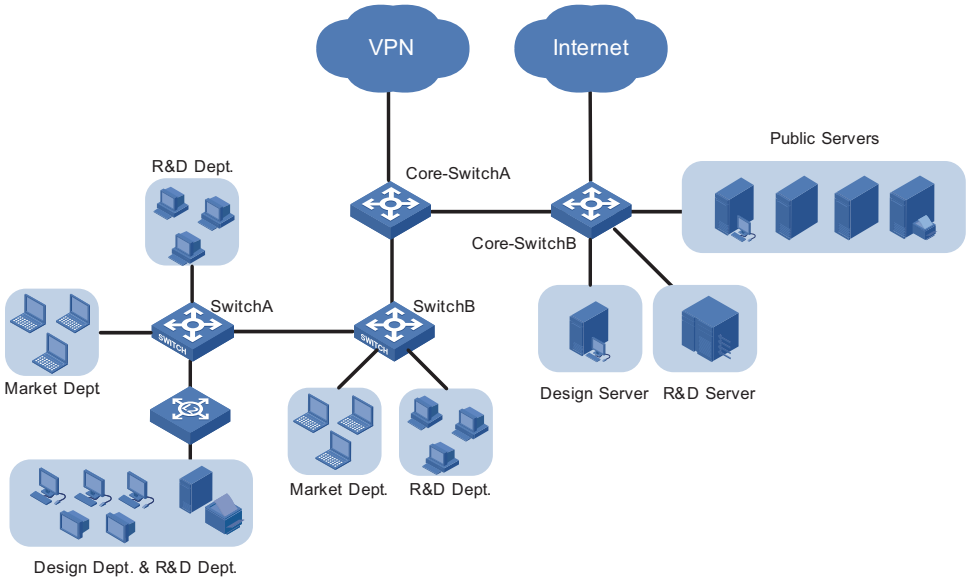
Network Requirements

A company has three departments: the R&D department, the marketing department, and the design department. The three departments are located in the same building. The R&D department and the marketing department are located in different office areas. The design department and part of the R&D department share the same office area. The hosts of the design department use the Apple operating system (OS), and the hosts of the other two departments use Windows. Use VLANs to fulfill the following:

- Employees of the same department can communicate with each other, while employees of different departments cannot.
- The R&D department and the marketing department are on different IP network segments. A switch (Core-Switch A in Figure 71) assigns addresses to hosts of the two departments automatically.
- Both the R&D department and the marketing department can access the public servers. However, the design server and the R&D server are accessible to only the employees of the design department and the R&D department respectively.
- The hosts and server of the R&D department and those of the design department cannot access the Internet; the hosts and server of the marketing department and those of the design department cannot access the VPN of the R&D department.

Network Diagram

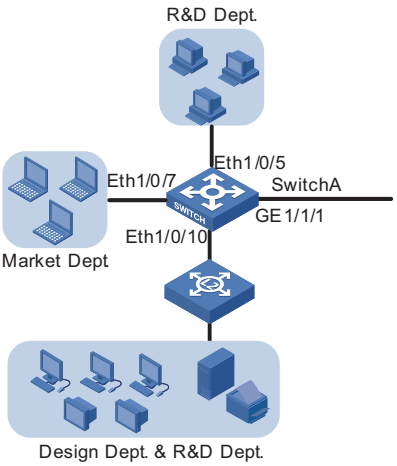
Figure 71 Network diagram for VLAN configuration



Configuration Outlines

Configuration on Switch A

Figure 72 Network diagram for Switch A



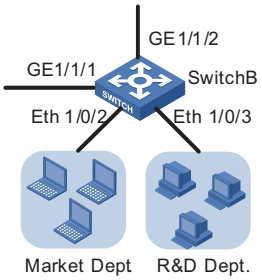
On Switch A, assign the port connecting to the independent office area of the R&D department and the port connecting to the independent office area of the marketing department to different VLANs, thus isolating the two areas.

As the shared office area is used by two departments, assigning the port connecting to the area to a VLAN cannot isolate the two departments. Considering that the design department and the R&D department use different operating systems, you can assign Apple hosts whose network protocol is Appletalk and Windows hosts whose network protocol is IP to different protocol VLANs.

Configure GigabitEthernet 1/1/1 to permit frames of all existing VLANs to pass through with VLAN tags for VLAN identification.

Configuration on Switch B

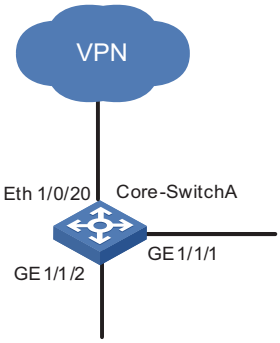
Figure 73 Network diagram for Switch B



On Switch B, assign the port connecting to the marketing department and the port connecting to the R&D department to different VLANs. Note that, the configuration of the VLAN to which a department belongs must be the same on both Switch A and Switch B. Configure the port connecting to Core-Switch A to permit the frames of all existing VLANs to pass through with VLAN tags.

Configuration on Core-Switch A

Figure 74 Network diagram for Core-Switch A

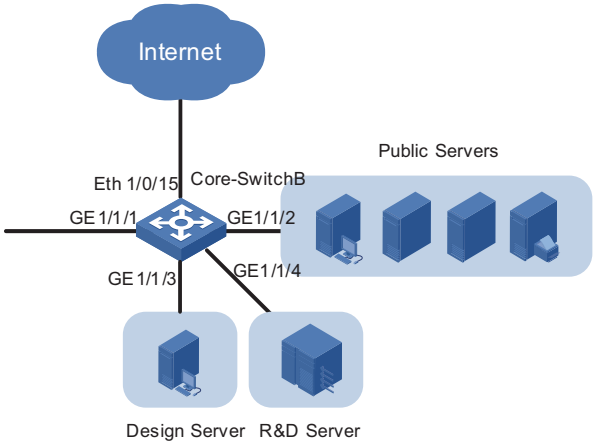


On Core-Switch A, configure the port connecting to Switch B to permit the frames of the three departments to pass through.

Configure Core-Switch A as the DHCP server for IP address assignment. As it is the egress device for the R&D department to access the VPN, configure Core-Switch A as the gateway for the R&D department and configure the port connecting to the VPN to permit only the frames of the R&D department to pass through. As Core-Switch B is the egress device for accessing the Internet and only the marketing department is allowed to access the Internet, configure Core-Switch B as the gateway for the marketing department.

Configuration on Core-Switch B

Figure 75 Network diagram for Core-Switch B



Each server is connected to Core-Switch B through an individual port. Assign these ports to different VLANs to provide the departments exclusive access to their respective servers.

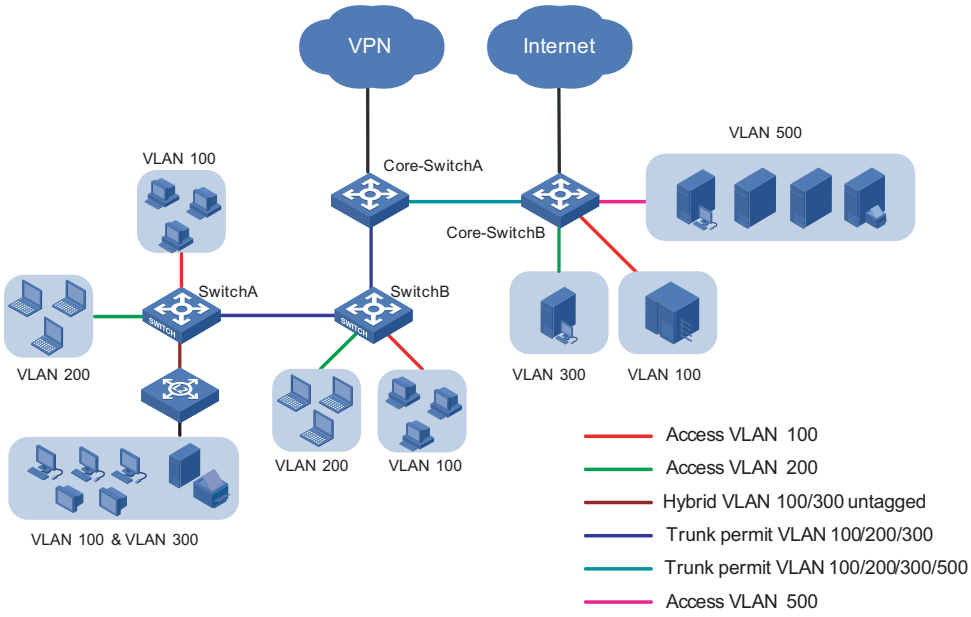
As the public servers are accessible to both the R&D department and the marketing department, create an individual VLAN for the public servers to forward Layer 3 traffic between the servers and the clients. As Core-Switch A forwards Layer 3 traffic between the R&D department and the public servers, configure the link between Core-Switch B and Core-Switch A to permit the frames of the VLAN created for the public servers to pass through besides the frames of the three departments.

As Core-Switch B is the egress device for accessing the Internet and only the marketing department is allowed to access the Internet, configure a VLAN interface with an IP address for the VLAN of the marketing department and configure the port connecting to the Internet to permit only the frames of the VLAN to pass through. The IP address of the VLAN interface will be used as the gateway address for the marketing department on Core-Switch A.

Summary

Assign the hosts and server of the R&D department, those of the marketing department, and those of the design department to VLAN 100, VLAN 200, and VLAN 300 respectively. The public servers belong to VLAN 500 and lie on the network segment 192.168.50.0. The following diagram shows the planned VLANs:

Figure 76 Network diagram for the deployment of VLANs



Configuration Procedure

Device and version used

Switch 5500 Release version V03.02.04.

Configuration procedure

- Configure Switch A

Create VLAN 100, VLAN 200, and VLAN 300.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
[SwitchA] vlan 300
[SwitchA-vlan300]
[SwitchA-vlan300] quit
```

Assign Ethernet 1/0/5 to VLAN 100.

```
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Ethernet1/0/5] port access vlan 100
[SwitchA-Ethernet1/0/5] quit
```

Assign Ethernet 1/0/10 to VLAN 200.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port access vlan 200
[SwitchA-Ethernet1/0/10] quit
```

Create a protocol template for VLAN 100 to carry IP and a protocol template for VLAN 300 to carry Appletalk.

```
[SwtichA] vlan 100
[SwitchA-vlan100] protocol-vlan ip
[SwitchA-vlan100] quit
[SwitchA] vlan 300
[SwitchA-vlan300] protocol-vlan at
[SwitchA-vlan300] quit
```

Create a user-defined protocol template for VLAN 100 to carry ARP for IP communication, assuming that Ethernet_II encapsulation is used.

```
[SwitchA] vlan 100
[SwitchA-vlan100] protocol-vlan mode ethernetii etype 0806
```

Configure Ethernet 1/0/10 as a hybrid port permitting the frames of VLAN 100 and VLAN 300 to pass through untagged.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link hybrid
[SwitchA-Ethernet1/0/10] port hybrid vlan 100 300 untagged
```

Associate Ethernet 1/0/10 with all the protocol templates of VLAN 100 and VLAN 300.

```
[SwitchA-Ethernet1/0/10] port hybrid protocol-vlan vlan 100 all
[SwitchA-Ethernet1/0/10] port hybrid protocol-vlan vlan 300 all
[SwitchA-Ethernet1/0/10] quit
```

Configure GigabitEthernet 1/1/1 as a trunk port permitting the frames of VLAN 100, VLAN 200, VLAN 300, and VLAN 500 to pass through with VLAN tags.

```
[SwitchA] interface GigabitEthernet 1/1/1
[SwitchA-GigabitEthernet1/1/1] port link-type trunk
[SwitchA-GigabitEthernet1/1/1] port trunk permit vlan 100 200 300 500
```

- Configure Switch B

Create VLAN 100, VLAN 200, and VLAN 300 on Switch B as you have done on Switch A.

Assign Ethernet 1/0/2 and Ethernet 1/0/3 to VLAN 200 and VLAN 100 respectively.

```
<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port access vlan 200
[SwitchB-Ethernet1/0/2] quit
[SwitchB] interface Ethernet 1/0/3
[SwitchB-Ethernet1/0/3] port access vlan 100
[SwitchB-Ethernet1/0/3] quit
```

Configure GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 as trunk ports permitting the frames of VLAN 100, VLAN 200, VLAN 300, and VLAN 500 to pass through with VLAN tags.

```
[SwitchB] interface GigabitEthernet 1/1/1
[SwitchB-GigabitEthernet1/1/1] port link-type trunk
[SwitchB-GigabitEthernet1/1/1] port trunk permit vlan 100 200 300 500
[SwitchB-GigabitEthernet1/1/1] quit
```

```
[SwitchB] interface GigabitEthernet 1/1/2
[SwitchB-GigabitEthernet1/1/2] port link-type trunk
[SwitchB-GigabitEthernet1/1/2] port trunk permit vlan 100 200 300 500
[SwitchB-GigabitEthernet1/1/2] quit
```

- Configure Core-Switch A

Create VLAN 100, VLAN 200, and VLAN 300 on Core-Switch A. The configuration procedure is the same as that on Switch A.

Configure GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 as trunk ports permitting the frames of VLAN 100, VLAN 200, VLAN 300, and VLAN 500 to pass through with VLAN tags. The configuration procedure is the same as that on Switch B.

Create VLAN-interface 100 and assign it IP address 192.168.30.1. Use this address as the IP address of the gateway for the R&D department. Allocate IP addresses in the address pool 192.168.30.0/24 for the hosts of the R&D department.

```
[Core-SwitchA] dhcp enable
[Core-SwitchA] interface Vlan-interface 100
[Core-SwitchA-Vlan-interface100] ip address 192.168.30.1 24
[Core-SwitchA-Vlan-interface100] dhcp select interface
[Core-SwitchA-Vlan-interface100] quit
```

Create a global IP address pool **mk** with the address segment 192.168.40.0/24 to allocate IP addresses for the hosts of the marketing department. Configure the gateway IP address as 192.168.40.1 for the hosts, pointing to Core-Switch B.

```
[Core-SwitchA] dhcp server ip-pool mk
[Core-SwitchA-dhcp-pool-mk] network 192.168.40.0 mask 255.255.255.0
[Core-SwitchA-dhcp-pool-mk] gateway-list 192.168.40.1
```

For detailed information about configuring DHCP, refer to the Switch 5500 Family Configuration Guide.

Create VLAN 500 and VLAN-interface 500 on Core-Switch A and assign IP address 192.168.50.1/24 to VLAN-interface 500. Configure the trunk port GigabitEthernet 1/1/1 to carry VLAN 500 and configure GigabitEthernet 1/1/1 to permit the frames of VLAN 500 to pass through with VLAN tags.

```
[Core-SwitchA] vlan 500
[Core-SwitchA-vlan500] quit
[Core-SwitchA] interface Vlan-interface 500
[Core-SwitchA-Vlan-interface500] ip address 192.168.50.1 24
[Core-SwitchA-Vlan-interface500] quit
[Core-SwitchA] interface GigabitEthernet 1/1/1
[Core-SwitchA-GigabitEthernet1/1/1] port trunk permit vlan 500
```

Create a VLAN-interface on Core-Switch A to forward traffic of the R&D department to the VPN and assign an IP address to the VLAN-interface. Assign Ethernet 1/0/20 to the VLAN corresponding to the VLAN-interface. The configuration procedure is omitted here.

- Configuration on Core-Switch B

Create VLAN 100, VLAN 200, VLAN 300, and VLAN 500 on Core-Switch B. The configuration procedure is the same as that on Switch A.

Configure GigabitEthernet 1/1/1 as a trunk port permitting the frames of all existing VLANs to pass through with VLAN tags. The configuration procedure is omitted here.

Create a VLAN-interface on Core-Switch B to forward traffic of the marketing department to the Internet and assign an IP address to the VLAN-interface. Assign Ethernet 1/0/15 to the VLAN corresponding to the VLAN-interface. The configuration procedure is omitted here.

Configure GigabitEthernet 1/1/3 and GigabitEthernet 1/1/4 to permit only the frames of VLAN 300 and only the frames of VLAN 100 to pass through respectively.

Configure GigabitEthernet 1/1/2 to permit only the frames of VLAN 500 to pass through.

Assign IP address 192.168.40.1 to VLAN-interface 200. The configuration procedure is omitted here.

Configuration remarks

After you finish the configuration, the hosts of the three departments should be isolated at the data link layer.

As no VLAN interface is created for the VLAN of the marketing department on the VPN gateway Core-Switch A, the hosts of the marketing department should not be able to access the VPN or the R&D department through Layer 3 forwarding. Similarly, as no VLAN interface is created for the VLAN of the R&D department on the Internet gateway Core-Switch B, the hosts of the R&D department should not be able to access the Internet or the marketing department through Layer 3 forwarding.

Thus, all departments are isolated at both the data link layer and the network layer.

To prevent users from modifying the IP addresses and gateways of hosts for accessing unauthorized network resources, you are recommended to enable DHCP-Snooping on Switch A and Switch B to monitor the IP addresses of clients. For detailed information about configuring DHCP-Snooping, refer to the Switch 5500 Family Configuration Guide.

Precautions

- Because IP depends on ARP for address resolution in Ethernet, you are recommended to configure the IP and ARP templates in the same VLAN and associate them with the same port to prevent communication failure.
- The maximum number of protocol templates that can be bound to a port varies by device.

Protocols and Standards

IEEE 802.1Q: *Virtual Bridged Local Area Networks*

8 VLAN CONFIGURATION EXAMPLES

Keywords:

VLAN, 802.1q, voice VLAN

Abstract:

This document introduces how voice VLAN of the 3Com series Ethernet switches is applied and configured in a network.

Acronyms:

VLAN (Virtual local area network)

Voice VLAN Support Matrix

In the 3Com series Ethernet switches based on the Comware V3.10 software platform, the following models support voice VLAN:

- Switch 5500
- Switch 5500G
- Switch 4500
- Switch 4200
- E352/E328
- Switch 4210
- E126A

Configuring Voice VLAN

- *For how to configure VLAN, port type and other related functions that voice VLAN configuration involves, refer to the configuration guide that applicable to your switch.*
- *The configuration procedure differs by device. This configuration example uses the Switch 5500. For information on how to configure voice VLAN on other switches, refer to the Configuration Guide for that model.*
- *The configuration example in this guide provides only basic configuration procedures. For detailed information about the involved functions, refer to the switch's configuration guide and command reference guide.*

Configuring a Voice VLAN in automatic mode

Follow these steps to configure a voice VLAN in automatic mode:

To...	Use the command...	Remarks
Enter system view	**system-view**	-

To...	Use the command...	Remarks
Add a recognizable voice device vendor OUI to the OUI address list	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the switch identifies voice traffic according to the default OUI address list.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional Enabled by default.
Set the voice VLAN aging time	**voice vlan aging** *minutes*	Optional 1440 minutes by default.
Enable voice VLAN globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable voice VLAN on the port	**voice vlan enable**	Required Disabled by default.
Enable voice VLAN legacy on the port to allow for automatic voice VLAN assignment for voice traffic from third-party vendors' voice devices	**voice vlan legacy**	Optional Disabled by default.
Configure the voice VLAN to operate in automatic mode on the port	**voice vlan mode auto**	Optional Automatic mode applies by default.

Configuring a Voice VLAN in manual mode

Follow these steps to configure a voice VLAN in manual mode:

To...	Use the command...	Remarks
Enter system view	**system-view**	-
Add a recognizable voice device vendor OUI to the OUI address list	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the switch identifies voice traffic according to the default OUI address list.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional Enabled by default.
Set the voice VLAN aging time	**voice vlan aging** *minutes*	Optional 1440 minutes by default.
Enable voice VLAN globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable voice VLAN on the port	**voice vlan enable**	Required Disabled by default.
Enable voice VLAN legacy on the port to allow for automatic voice VLAN assignment for voice traffic from third-party vendors' voice devices	**voice vlan legacy**	Optional Disabled by default.

To...			Use the command...	Remarks
Configure the voice VLAN to operate in manual mode on the port			**undo voice vlan mode auto**	Required Automatic mode applies by default.
Return to system view			**quit**	-
Assign the port to the voice VLAN	Access port	Enter VLAN view	**vlan** *vlan-id*	Required
		Assign the specified port(s) to the VLAN	**port** *interface-list*	
	Trunk port or hybrid port	Enter port view	**interface** *interface-type interface-number*	
		Assign the port to the specified VLAN	**port trunk permit vlan** *vlan-id* **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
		Configure the voice VLAN as the default VLAN of the port	**port trunk pvid vlan** *vlan-id* **port hybrid pvid vlan** *vlan-id*	Optional

Voice VLAN Configuration Examples

A company plans to deploy IP phones in the office area and meeting rooms. To guarantee voice quality, the voice traffic must be transmitted in a VLAN dedicated to voice traffic. At the same time, assign different network segments for the IP phones in the meeting rooms and those in the office area.

- Network requirements of the IP phones in the office area

All IP phones can get an IP address and voice VLAN information automatically. In addition, they can send tagged voice traffic. The IP phones connect to a switch port via the PCs of their users. It is required that the switch port exit the voice VLAN automatically if no voice traffic has passed by within 100 minutes.

- Network requirements of the IP phones in the meeting rooms

The company deploys IP phones in two meeting rooms. The IP phone in meeting room 1 sends VLAN untagged voice traffic. The OUI address of the IP phone is 00e3-f200-0000. In addition, the IP address of the IP phone is manually configured. In meeting room 2, a Cisco IP phone capable of getting an IP address and voice VLAN information automatically is deployed. The IP phone sends VLAN tagged voice traffic.

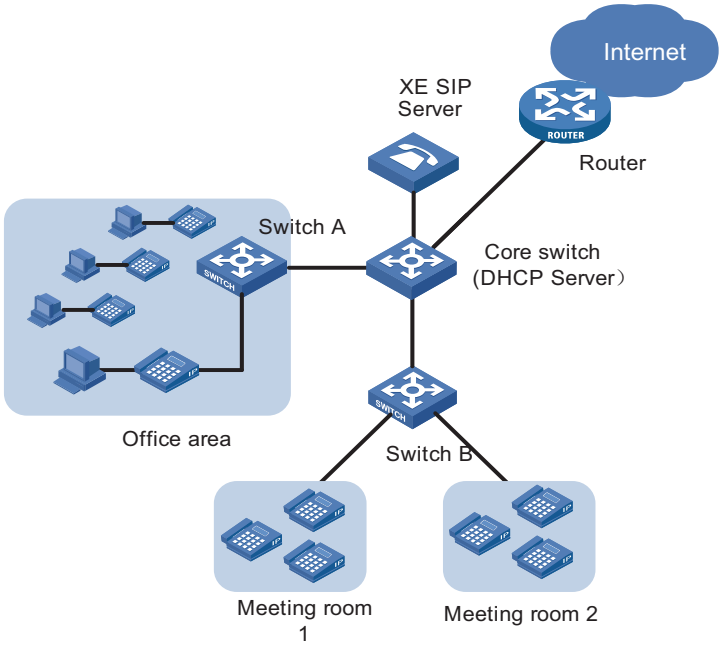
- Overall network requirements

The IP phones and PCs in the office area connect to the enterprise network through Switch A, and the IP phones in the two meeting rooms connect to the enterprise network via Switch B. The two switches and an XE voice server are connected to the core switch. The core switch connects to the Internet through an egress router. In addition, the core switch also operates as the DHCP server to

allocate IP addresses and voice VLAN configuration for the IP phones configured to get IP addresses automatically.

Network Diagram

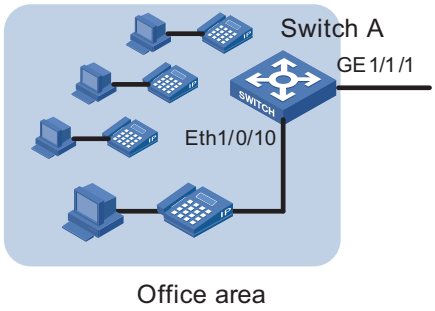
Figure 77 Network diagram for voice VLAN configuration



Configuration Outlines

Configuration on Switch A

Figure 78 Network diagram for Switch A



As the IP phones connected to Switch A get IP addresses automatically, they should send an untagged DHCP request to the DHCP server for an IP address upon their startup. When the DHCP server receives a request, it responds with a temporary IP address, and in addition, the voice VLAN ID, and the IP address of the voice server. After the IP phone receives the response, it discards the temporary IP address and re-sends a DHCP request with the voice VLAN tag to the DHCP server. Thus, the IP phone gets an IP address within the voice VLAN to communicate with the voice server normally.

The above procedure describes how a common IP phone gets an IP address. The procedure may differ depending on your IP phone. For the actual procedure of your IP phone, refer to its user manual.

In this network, as Ethernet 1/0/10 of Switch A is required to forward traffic of the default VLAN and the voice VLAN, you should configure Ethernet 1/0/10 as a trunk port or hybrid port. In this example, Ethernet 1/0/10 is configured as a hybrid port. As the traffic from the PCs is untagged, it will be transmitted through the default VLAN. Configure VLAN 100 as the default VLAN and configure the port to transmit the traffic of the default VLAN untagged. As the IP phones send tagged traffic after getting IP addresses within the voice VLAN, configure VLAN 200 as the voice VLAN and configure the voice VLAN to operate in automatic mode on the port. Thus, the port can join/exit the voice VLAN automatically.

A hybrid port with voice VLAN enabled in automatic mode joins the voice VLAN in tagged mode automatically and sends the traffic of the voice VLAN tagged.

On Switch A, GigabitEthernet 1/1/1 is uplinked to the core switch to transmit both service traffic and voice traffic. To discriminate data, configure the port as a trunk port to carry VLAN 100 and VLAN 200. As the switch is required to send traffic of the two VLANs tagged, do not configure either of them as the default VLAN.

Figure 77 lists the port configurations on Switch A.

Table 89 Port configurations on Switch A

Port	Voice VLAN mode	Port type	Permitted VLANs and operations on the VLAN traffic
Ethernet 1/0/10	Automatic mode	Trunk/hybrid	VLAN100: pvid, untagged
GigabitEthernet 1/1/1	-	Trunk	VLAN100: tagged VLAN200: tagged

The following describes the operations on VLAN traffic

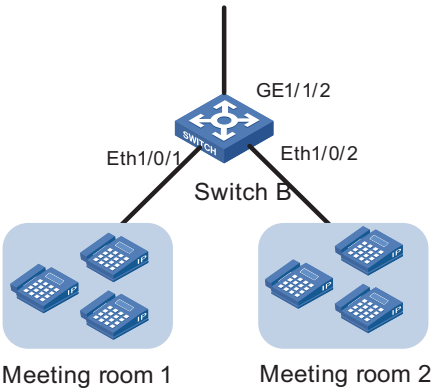
- *pvid: Indicates that the VLAN is configured as the default VLAN of the port.*
- *untagged: Indicates that the port sends the traffic of the VLAN untagged.*
- *tagged: Indicates that the port sends the traffic of the VLAN tagged.*

For instructions on configuring the port's default VLAN and configuring the port to send traffic untagged or tagged, refer to the applicable configuration guideconfiguration guide.

In this configuration, Ethernet 1/0/10 is configured as a hybrid port.

Configuration on Switch B

Figure 79 Network diagram for Switch B



As two types of IP phones are connected to Switch B, the configuration on Ethernet 1/0/1 is different from that on Ethernet 1/0/2.

- Ethernet 1/0/1

The IP phones connected to Ethernet 1/0/1 are configured with an IP address manually and they send voice traffic untagged. As the port with the voice VLAN mode set to auToes not support receiving untagged voice traffic, you should configure the voice VLAN to operate in manual mode on the port. In addition, configure the voice VLAN as the default VLAN of the port.

- Ethernet 1/0/2

You can configure Ethernet 1/0/2 in a way similar to configuring Ethernet 1/0/10 on Switch A. However, because only IP phones are connected to Ethernet 1/0/2, you can assign the port to the voice VLAN manually to guarantee stable transmission for voice traffic. For the Cisco IP phones connected to the port to communicate with the switch, enable voice VLAN legacy on the port to notify them of the voice VLAN ID, so that the Cisco IP phones can request IP addresses within the voice VLAN. Because the IP phones send tagged voice traffic, you should configure the port to send the traffic of the voice VLAN tagged.

- GigabitEthernet 1/1/2

The port sends the voice traffic received on Switch B. As the meeting rooms should use a voice VLAN different from that for the office area, configure VLAN 400 as the voice VLAN on Switch B and configure the port to send the traffic of VLAN 400 tagged.

Table 90 lists the port configurations on Switch B.

Table 90 Port configurations on Switch B

Port	Voice VLAN mode	Port type	Permitted VLANs and operations on the VLAN traffic
Ethernet 1/0/1	Manual mode	Access/hybrid/trunk	VLAN400: pvid untagged
Ethernet 1/0/2	Manual mode	Trunk/hybrid	VLAN400: tagged

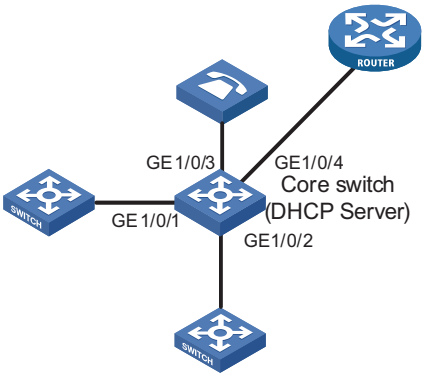
Table 90 Port configurations on Switch B

Port	Voice VLAN mode	Port type	Permitted VLANs and operations on the VLAN traffic
GigabitEthernet 1/1/2	-	Trunk/hybrid	VLAN400: tagged

In this configuration, Ethernet 1/0/1 is configured as an access port, and Ethernet 1/0/2 and GigabitEthernet 1/1/2 are configure as trunk ports.

Configuration on Core Switch

Figure 80 Network diagram for the Core Switch



The core switch forwards traffic, allocates IP addresses to IP phones, and specifies the voice VLAN and the voice server address.

According to the configuration on Switch A and Switch B, the core switch is required to forward the traffic of VLAN 100, VLAN 200, and VLAN 400, and allocate IP addresses to IP phones in VLAN 200 and VLAN 400.

As analyzed earlier, when an IP phone is powered up, it first gets an IP address in the default VLAN (VLAN 100) from the DHCP server. The DHCP server should return not only an IP address but also the voice VLAN and the voice server address to the IP phone. To achieve that, you should configure the core switch to use option 184 in the DHCP responses in VLAN 100 for conveying voice related information.

After the IP phone gets the voice VLAN information, it requests for an IP address in the voice VLAN instead of using the IP address obtained in the default VLAN. When receiving the request, the core switch allocates an IP address in VLAN 200 or VLAN 400, whichever the IP phone belongs to. Note that VLAN 200 and VLAN 400 use different IP address segments.

As both the XE voice server and the egress router are connected to the core switch, you should create two VLAN interfaces, and assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to the two VLANs respectively, thus achieving Layer-3 forwarding.

Table 91 lists the interface and port configurations on the core switch.

Table 91 Interface and port configurations on the core switch

VLAN interface	IP address and network segment	Ports involved	Port type	Operations on the VLAN traffic
Vlan-interface100	192.168.1.1/24	GigabitEthernet 1/0/1	Trunk	tagged
Vlan-interface200	192.168.2.1/24	GigabitEthernet 1/0/1	Trunk	tagged
Vlan-interface400	192.168.4.1/24	GigabitEthernet 1/0/2	Trunk	tagged
Vlan-interface300	192.168.3.1/24	GigabitEthernet 1/0/3	Access	untagged
Vlan-interface500	192.168.5.1/24	GigabitEthernet 1/0/4	Access	untagged

Configuration Procedure

Devices and software version used

Switch A and Switch B are Switch 5500s with software version Release V03.02.04. The core switch is a Switch 5500Gs Ethernet switch whose software version is V03.02.04.

Configuration steps

Switch A Configuration

Create VLAN 100 and VLAN 200.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
```

Assign GigabitEthernet 1/1/1 and Ethernet 1/1/10 to the specified VLANs according to Table 89.

```
[SwitchA] interface GigabitEthernet 1/1/1
[SwitchA-GigabitEthernet1/1/1] port link-type trunk
[SwitchA-GigabitEthernet1/1/1] port trunk permit vlan 100 200
[SwitchA-GigabitEthernet1/1/1] quit
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type hybrid
[SwitchA-Ethernet1/0/10] port hybrid vlan 100 untagged
[SwitchA-Ethernet1/0/10] port hybrid pvid vlan 100
[SwitchA-Ethernet1/0/10] quit
```

Enable voice VLAN on Ethernet 1/0/10.

```
[SwitchA-Ethernet1/0/10] voice vlan enable
```

Set the voice VLAN aging time to 100 minutes.

```
[SwitchA-Ethernet1/0/10] quit
[SwitchA] voice vlan aging 100
```

Enable voice VLAN security mode so that only voice traffic is transmitted in the voice VLAN. (Optional. The voice VLAN security mode is enabled by default.)

```
[SwitchA] voice vlan security enable
```

Configure VLAN 200 as the voice VLAN globally.

```
[SwitchA] voice vlan 200 enable
```

- Configuration on Switch B

Create VLAN 100 and VLAN 400.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] vlan 400
[SwitchB-vlan400] quit
```

Assign Ethernet 1/0/1, Ethernet 1/0/2, and GigabitEthernet 1/1/2 to the specified VLANs according to Table 90.

```
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port access vlan 400
[SwitchB-Ethernet1/0/1] quit
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type trunk
[SwitchB-Ethernet1/0/2] port trunk permit vlan 100 400
[SwitchB-Ethernet1/0/2] quit
[SwitchB] interface GigabitEthernet1/1/2
[SwitchB-GigabitEthernet1/1/2] port link-type trunk
[SwitchB-GigabitEthernet1/1/2] port trunk permit vlan 100 400
[SwitchB-GigabitEthernet1/1/2] quit
```

Enable voice VLAN legacy on Ethernet 1/0/2.

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] voice vlan legacy
[SwitchB-Ethernet1/0/2] quit
```

Configure the voice VLAN to operate in manual mode on Ethernet 1/0/1 and Ethernet 1/0/2, and enable voice VLAN on the two ports.

```
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] undo voice vlan mode auto
[SwitchB-Ethernet1/0/1] voice vlan enable
[SwitchB-Ethernet1/0/1] quit
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] undo voice vlan mode auto
[SwitchB-Ethernet1/0/2] voice vlan enable
[SwitchB-Ethernet1/0/2] quit
```

Add an OUI address 00e3-f200-0000 with the description of **Meeting room1** globally.

```
[SwitchB] voice vlan mac-address 00e3-f200-0000 mask ffff-ff00-0000
description Meeting room1
```

Enable voice VLAN security mode so that only voice traffic is transmitted in the voice VLAN. This step is optional. The voice VLAN security mode is enabled by default.

```
[SwitchB] voice vlan security enable
```

Configure VLAN 400 as the voice VLAN globally.

```
[SwitchB] voice vlan 400 enable
```

Configure the core switch

Create VLAN 100, VLAN 200, VLAN 300, VLAN 400, and VLAN 500 on the core switch. Assign the specified ports to their respective VLANs according to Table 91. The configuration procedure is omitted here.

Create VLAN interfaces and assign IP addresses to the VLAN interfaces according to Table 91. The configuration procedure is omitted here.

Enable DHCP globally.

```
<CoreSwitch> system-view
[CoreSwitch] dhcp enable
```

Create a global address pool **vlan100** to allocate IP addresses on the network segment 192.168.1.1/24 to devices in the default VLAN (VLAN 100).

```
[CoreSwitch] dhcp server ip-pool vlan100
[CoreSwitch-dhcp-pool-vlan100] network 192.168.1.0 mask 255.255.255.0
```

Configure VLAN 200 as the voice VLAN and the voice server IP address as 192.168.3.3 for option 184 in the address pool **vlan100**.

```
[CoreSwitch-dhcp-pool-vlan100] voice-config ncp-ip 192.168.3.3
[CoreSwitch-dhcp-pool-vlan100] voice-config voice-vlan 200 enable
[CoreSwitch-dhcp-pool-vlan100] quit
```

Configure VLAN-interface 100 to operate in global address pool mode.

```
[CoreSwitch] interface Vlan-interface 100
[CoreSwitch-Vlan-interface100] dhcp select global
[CoreSwitch-Vlan-interface100] quit
```

Create an address pool for VLAN-interface 200 and VLAN-interface 400 respectively to allocate IP addresses for the IP phones in the office area and the IP phone in meeting room 2.

```
[CoreSwitch] interface Vlan-interface 200
[CoreSwitch-Vlan-interface200] dhcp select interface
[CoreSwitch-Vlan-interface200] quit
[CoreSwitch] interface Vlan-interface 400
[CoreSwitch-Vlan-interface400] dhcp select interface
```

For detailed information about configuring DHCP, refer to the Switch 5500 Family Configuration Guide.

The core switch thus configured should be able to allocate IP addresses, voice VLANs, and the voice server IP address for IP phones in VLAN 200 and VLAN 400, and to forward voice traffic at Layer 3. If required, configure dynamic routing protocols on the core switch, which is beyond the scope of this document.

Configuration remarks

After you finish the configuration, the IP phones in each area can establish connections with the voice server, get telephone numbers, and communicate normally. For the configuration on the voice server, refer to the NCP Network Call Processor documentation.

You are recommended to enable DHCP snooping and some security functions on Switch A and Switch B to ensure that only legal IP phones that get IP addresses from the core switch can use the service, thus preventing malicious interception.

Protocols and Standards

IEEE 802.1Q: *Virtual Bridged Local Area Networks*