N6000 Series/S4600/S2100P/S3600 Series/S3200P Series/S2200 Series

Configuration Guides

Foreword

Overview

This document presents the supported features and related configurations of Layer 3 Ethernet switches. The main content includes the fundamental principles and configuration process of basic hardware and software, Ethernet, ring protection, IP business, IP routing, reliability, safety, QoS, and IPV6 with related configuration examples. The appendixes to this document provide terms and abbreviations involved here.

The document helps readers to grasp devices' theories and configuration information, and the way to network with the devices.

The document applies to the following switches series models, including:

Data center N6000 Series (includingN6400H/N6100-48X8C/N6300-48Y8C/N6300-32C)

Campus network S4600 Series (S4600-24X2C), S3600 Series (including S3600-48S4X/S3600-24T24S4X), S3200P Series (including S3200P-24T4X/S3200P-48T4X), S2200 Series (including S2200-24T4X/S2200-48T4X), S2100 Series(including S2100P-8T2S)

Note: The supported features vary from product to product. Please refer to the actual features of products.

Stipulations

Symbol Stipulations

The following symbols may appear in the document, of which the meanings are as below.

Symbol	Description
	Text marked with this symbol means potential risk that may cause personal injury if it is cannot be avoided.
	Text marked with this symbol means potential risk that may cause equipment trouble, data loss, device performance degradation or unpredictable results if it is ignored.
	Text marked with this symbol delivers additional information to the body for emphasizing and complementing.

Symbol	Description
 TIP	Text marked with this symbol may help you address certain issues or save your time.

General Format Stipulations

Format	Description
Song	The main body is in Song.
Gothic	Level 1 title, Level 2 title, Level 3 title and Block are in Gothic.
Regular	Warnings and hints are in Regular.
“Lucida Console” format	“Lucida Console” format indicates screen output. Additionally, the data input by users from terminal among the screen output is displayed in bold font.

Command Line Format Stipulations

Format	Description
Boldface	Command line keywords (must be copied) are displayed in **Boldface**.
Italic	Command line parameters (must be replaced with a real value) are displayed in *Italic*.
[ ]	Means the content enclosed with “[ ]” is optional for command configuration.
{ x | y | ... }	Means selecting one from two or more options.
[x | y | ...]	Means selecting one or zero option from two or more options.
{ x | y | ... } *	Means selecting multiple options from two or more options, ranging from one to all.
[x | y | ...] *	Means selecting multiple options or zero option from two or more options.

Contents

1 Basic Configuration Guide

1.1 System Management Configuration

1.1.1 Introduction

Both MOTD (message-of-the-day) information and login prompt are configurable and can be displayed to all login users. If a user has an inappropriate operation that may affect all online users, it is necessary to send prompts to the user (such as logoff). Login prompt appears at the time terminal users logging in.

1.1.2 Configure Message Banner

Users can create one or more prompts that will appear on the terminal of login users. This feature can be configured as below.

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# banner motd c message c	Specify 255 character strings to the most
Switch(config)# exit	Exit configuration mode

1.1.3 Configure Login Banner

Users can configure one login prompt that display to all login users with the following steps.

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# banner login c message c	Specify 255 character strings to the most
Switch(config)# exit	Exit configuration mode

1.1.4 Configure Logout Banner

Users can configure one EXEC mode prompt that display to all users having logged in EXEC mode with the following steps.

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# banner exec c message c	Specify 255 character strings to the most
Switch(config)# exit	Exit configuration mode

1.1.5 Show BannerInformation

Show all current configurations

Switch1

Switch# show running	Show current configuration of the system

1.2 User Management Configuration

1.2.1 Overview

User management can be utilized for enhancing system security by requiring users to log in with password. The system will limit the number of login users. The switches are provided with three login modes: “no login” mode allows login to the switches without password; “login” mode allows default users to login only; “login local” mode requires users to create a user account to login to the switches. By creating a user account and password locally, users can login to the switches. 32 accounts are allowed for each switch only. Users must create an account before enabling local account authentication.

Users can set a unique password for each user name. User name of 32 characters or less is allowed.

Users can specify account level from 1 to 4. Only one account has access to configuration mode.

1.2.2 Configure User Level

Configure

Switch1

Switch# configure terminal	Enter configuration mode

Switch(config)# line vty 0 7	Enter user mode
Switch(config-line)# login local	Set authentication mode
Switch(config-line)# exit	Exit user mode
Switch(config)# username testname privilege 4 password 123abc<>	Create user name and password
Switch(config)# exit	Exit configuration mode

Command validation

With the above configurations, the following verification prompts will appear at the time of logging in switches:

Username: testname
Password:

1.2.3 Configure User Management

Log in with password with no user name.

Configure

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# line vty 0 7	Enter user mode
Switch(config-line)# login	Set authentication mode
Switch(config-line)# line-password abc	Set login password abc
Switch(config-line)# end	Exit user mode

Command validation

With the above configurations, the following verification prompts will appear at the time of logging in switches, and users can log in the switches with previously created password.

Password:

1.2.4 Steps of Password Recovery

The following steps help password recovery in case of password is forgotten.

Step 1 Connect switches via Console cord and power up.

CPU: MPC8247 (HiP7 Rev 14, Mask 1.0 1K50M) at 350 MHz
Board: 8247 (PCI Agent Mode)
I2C: ready

```
DRAM:  256 MB
In:    serial
Out:   serial
Err:   serial
Net:   FCC1 ETHERNET, FCC2 ETHERNET [PRIME]
Press ctrl+b to stop autoboot: 3
```

Step 2 Press **ctrl + b** to enter Uboot mode.

Step 3 According to the configurations below, the system will enter the switches normally.

Bootrom# boot_flash_nopass	Boot the system via an empty configuration file without password
Bootrom# Do you want to revert to the default config file ? [Y|N|E]:	Enter "Y"

1.3 FTP Configuration

1.3.1 Introduction

Users can download a switch configuration file from FTP server or upload files from switches to FTP server.

In the event of downloading a switch configuration file from FTP server to upgrade switch configuration, you need to overwrite the current startup configuration file with a new one. Switch configuration files can be uploaded to the server for backup, which can be downloaded to the original switch or similar switches for updating switch configuration in future, if necessary.

1.3.2 IPv4 Configuration

I. Make preparation to download or upload configuration files via FTP

Users can copy or upload files to FTP server.

FTP protocol requires FTP clients to send FTP request to the server with remote user name and password. Users must complete the following steps before uploading or downloading configuration file via FTP.

1. Make sure there is a reachable route between the switch and FTP server. If user's network is not capable of inter-subnet routing communication, the switch and FTP server must be in the same network. The connectivity of the FTP server can be checked via ping command.
2. If a user is accessing the switch via Console or Telnet, it should be ensured that the current FTP user name is valid and has access to FTP download function.
3. To upload configuration files to FTP server, users must configure FTP server correctly to accept the write request from switch users.

II. Download a configuration file via FTP

Users can download a new configuration file to overwrite the current configuration.

Switch1

Switch# configure terminal	Enter global configuration mode
Switch(config)# ftp username test	(Optional) create a user name“test”
Switch(config)# ftp password test	(Optional) create a password “test”
Switch(config)# end	Exit EXEC mode
Switch# copy mgmt-if ftp://test:test@10.10.10.163/ startup-config.conf flash:/startup-config.conf	Download a startup configuration file from remote FTP server with user name “test” and password “test”
Switch# show startup-config	Show configuration

III.Upload configuration files via FTP

Users can upload a configuration file from an FTP server and subsequently download the configuration from this switch or other switches.

Switch1

Switch# configure terminal	Enter global configuration mode
Switch(config)# ftp username test	(Optional) create a user name “test”
Switch(config)# ftp password test	(Optional) create a password “test”
Switch(config)# end	Exit EXEC mode
Switch# copy flash:/startup-config.conf mgmt-if ftp://test:test@10.10.10.163/startup-config.conf	Upload a configuration file to remote FTP server with user name “test” and password “test”

1.3.3 IPv6 Configuration

I. Download a configuration file via FTP

Switch1

Switch# copy ftp://root: root@2001:1000::2/startup-config.conf flash:/startup-config.conf	Download a startup configuration file from remote FTP server with user name “root” and password “root”

Switch# show startup-config	Show configuration

II.Upload configuration files via FTP

Switch1

Switch# copy flash:/startup-config.conf mgmt-if ftp://root:root@2001:1000::2 startup-config.conf	Upload a configuration file to remote FTP server with user name “root” and password “root”

1.4 TFTP Configuration

1.4.1 Overview

TFTP (Trivial File Transfer Protocol) is a protocol for trivial file transfer between client and server to render uncomplicated file transfer service that costs little, which belongs to TCP/IP protocol family. The port number is 69.

This protocol is designed for trivial file transfer. Therefore, it doesn't have many functions that FTP has, can fetch files from or in-file to file server only, cannot list the directory, cannot perform authentication, and transfers 8-bit data.

1.4.2 Configuration

I. Upload and download software via TFTP server

The following steps must be completed before uploading or downloading:

- Make sure the workstation that serves as TFTP server is configured correctly.
- Make sure the routability from the switch to TFTP server. If there is no router provided for routing communication between subnets, the switch and the TFTP server must be in the same network. The connectivity of the TFTP server can be checked via ping command.
- Make sure the configuration files to be downloaded are under the correct catalogue of the TFTP server.
- For downloading, it should be ensured that the file access is set correctly.
- For uploading, it should be ensured that the access setting of the file is correct if it is intended to overwrite the existing files (including empty file) on the server.

II. Download

Switch1

Switch# copy mgmt-if tftp://10.10.10.163/startup-config.conf flash:/startup-config.conf	Specify IPv4 address and corresponding files of TFTP server

Switch# copy mgmt-if tftp://2001:1000::2/startup-config.conf flash:/startup-config.conf	Specify IPv6 address and corresponding files of TFTP server
Switch# show startup-config	Check the downloaded files

Upload

Switch1

Switch# copy flash:/startup-config.conf mgmt-if tftp://10.10.10.163/startup-config.conf	Specify files to be uploaded and IPv4 address of the server
Switch# copy flash:/startup-config.conf mgmt-if tftp://2001:1000::2/startup-config.conf	Specify files to be uploaded and IPv6 address of the server

1.5 Telnet Configuration

1.5.1 Overview

Telnet protocol belongs to TCP/IP protocol family, and is a standard protocol and main way for Internet remote login service. It enables users to complete remote host login on local computer. Telnet program is used on the computer of terminal users to connect to server. Terminal users can input commands in Telnet program. The commands will run on the server as they are directly input from the console of the server. With Telnet program, users can control the server locally. To start a Telnet session, server login with user name and password must be completed. Telnet is a commonly used method of remote control over Web server.

1.5.2 Configuration

Step 1 Through in-band interface Telnet towards other switches.

Switch# telnet 10.10.29.247	Through in-band interface Telnet towards other switches
Switch# telnet 2001:1000::71	Through in-band interface Telnet towards other switches

Step 2 Through management interface Telnet towards other switches.

Switch# telnet mgmt-if 10.10.29.247	Through management interface Telnet towards other switches

Switch# telnet mgmt-if 2001:1000::2	Through management interface Telnet towards other switches

Step 3 The switch is also a Telnet server.

Switch# configure terminal	Enter configuration mode
Switch(config)# service telnet enable	Enable Telnet service

1.5.3 Command Validation

Switch# telnet mgmt-if 10.10.38.1

Entering character mode
Escape character is '^]'.
Switch #

Switch# telnet 2001:1000::71

Entering character mode
Escape character is '^]'.
Switch #

1.6 SSH Configuration

1.6.1 Overview

Security shell (SSH) is a protocol that can provide a secure environment for users for remote connection to devices. In the case of remote device access, SSH is more powerful in encryption than Telnet. SSH supports data encryption standard (DES) algorithm and triple DES (3DES) algorithm, and provides password-based user authentication.

1.6.2 Topology

Figure 1-1 SSH System Application

1.6.3 Configure

Create a KEY of SSH

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# rsa key a generate	Create a key
Switch(config)# rsa key a export url flash:/a.pri private ssh2	Take a.pri private key from Flash
Switch(config)# rsa key a export url flash:/a.pub public ssh2	Take a.pub public key from Flash

Import KEY

Switch1

Switch(config)# rsa key importKey import url flash:/a.pub public ssh2	Import a key named a.pub
Switch(config)# username aaa privilege 4 password abc	Create a user name aaa
Switch(config)# username aaa assign rsa key importKey	Specify SSH user name aaa

1.6.4 Command Validation

From SSH client

- Download a. pri key
- Load switches

[root@test1 tftpboot]# ssh -i a.pri aaa@10.10.39.101

aaa@10.10.39.101's password:
Switch #

1.7 NETCONF-SSH Configuration

1.7.1 Overview

Netconf feature depends on SSH-provided port-specific listening service, Port 830 by default. Enabling or disabling netconf feature is realized by controlling the enable/disable of SSH port 830 listening.

1.7.2 Topology

Figure 1-2 Netconf-SSH System Application

1.7.3 Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# netconf ssh enable	Enable ssh listening of netconf feature
Switch(config)# netconf ssh disable	Disable ssh listening of netconf feature

1.7.4 Command Validation

router# show run | include netconf

router# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

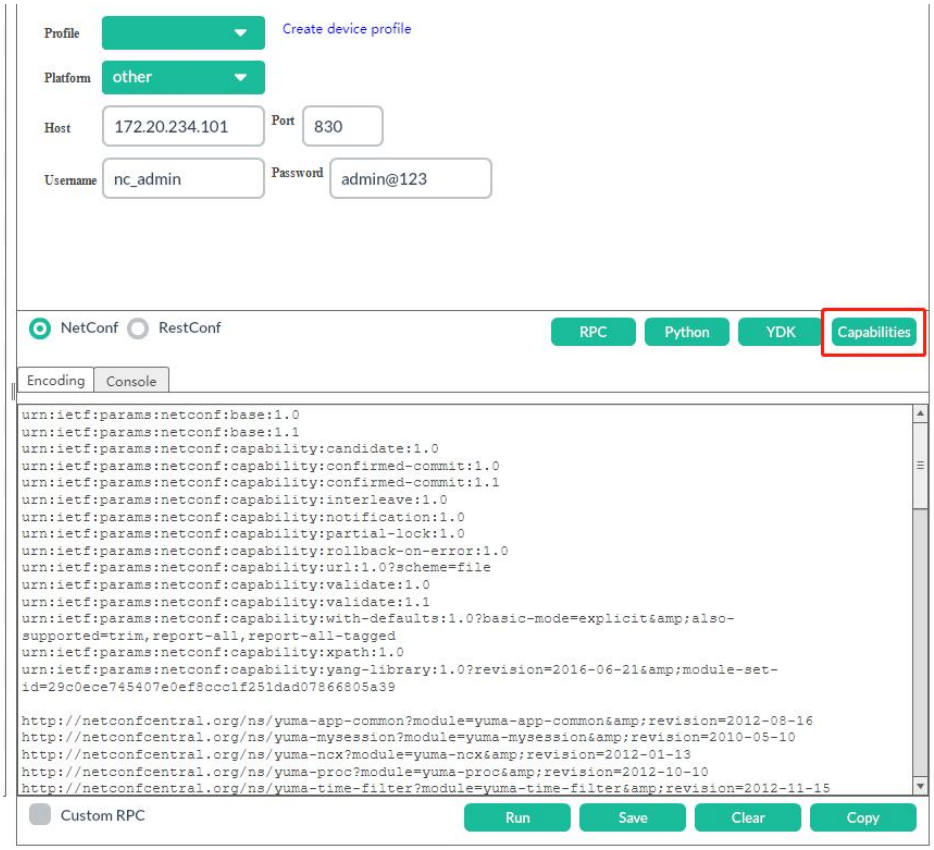
router(config)# netconf ssh enable

router(config)# exit

router# show run | include netconf

netconf ssh enable

Netconf protocol communication with switches can be achieved using third-party tool yang-explorer:



1.8 Time Configuration

1.8.1 Overview

To guarantee coordination with other devices, users must set the system time accurately. If no external time source is provided, you can set the time and date manually after startup. If you have other ways to synchronize time such as NTP, manual setup is not recommended.

1.8.2 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# clock set datetime 11:30:00 10 26 2013	Set system datetime
Switch(config)# clock set summer-time dst date 6 1 2013 02:00:00 10 31 2013 02:00:00 120	Set summer-time and time zone
Switch(config)# exit	Exit global configuration mode
Switch# show clock detail	Show clock detail

1.8.3 Command Validation

Switch# show clock detail

13:31:10 dst Sat Oct 26 2013
Time zone: (GMT + 08:00:00) beijing
Summer time starts at beijing 02:00:00 06/01/2013
Summer time ends at dst 02:00:00 10/31/2013
Summer time offset: 120 minutes

1.9 Certificate Configuration

1.9.1 Overview

The access to advanced features of switches requires certification authentication. Each switch has its unique certificates to avoid unknown errors due to utilization of advanced features by unauthorized users. Three types of certificate are provided: Enterprise Base, Metro Service, and Metro Advanced. The features vary with certificate type, and users can request a certificate as needed. A switch with no certificate can have access to L2 related features only.

The certificates are unsharable between switches. To be granted a certificate of a specific switch, the UDI of the switch must be generated first and then sent to the vendor for certificate request. After granting, apply it to the corresponding switch.

1.9.2 Configuration

Generate UDI

Switch# generate device identifier mgmt-if ftp://test:test@10.10.25.33/device.udi	Generate switch UDI and send it to FTP server

Certificate Request

Send UDI file to the vendor, and the vendor will generate the certificate as requested and send it to customer.

Certificate Usage

- Reboot the switch to validate the certificate.
- A switch with no valid certificate can have access to L2 related features only
- A switch with multiple certificates can have access to all features granted via the certificates.

Switch# copy mgmt-if ftp://test:test@10.10.25.33/device.lic flash:/device.lic	Copy the certificate from FTP server to local computer
Switch# reload	Reboot

1.9.3 Command Validation

Switch# show license

```
License files:
==========================================================================
flash:/ma.lic:
 Created Time:  Fri Dec  6 17:22:23 CST 2013
 Vendor:        centec
 Customer:      centec
 Device MAC:    00:1E:08:09:03:00
 Feature Set:   QINQ MVR ERPS MEF ETHOAM
                VPWS VPLS HVPLS SMLK TPOAM
                OSPF PIM_SM IGMP VRF MPLS
                 LDP BGP RSVP OSPF_TE EXTEND_ACL
                 PTP BFD SSM IPV6 OSPF6
                 PIM_SM6 MVR6 RIPNG TUNNEL_V6
```

2 Ethernet Configuration Guide

2.1 Interface Configuration

2.1.1 Introduction

Ethernet interfaces run at the speed of 10/100/1000 Mbps in full-duplex or half-duplex mode. Combo is for photoelectric multiplex. Users can choose one depending on the actual networking needs, but simultaneous working is not supported. While one interface is activated, the other is automatically disabled. With the combo interface operating in optical interface mode, speed configuration and duplex are invalid.

2.1.2 Interface Status Configuration

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch#(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# shutdown	Shut down interface eth-0-2
Switch(config)# end	Exit
Switch# show interface status	Show interface status

II. Command validation

Switch# show interface status

```
Port      Status    Duplex  Speed   Mode    Type
------------------------------------------------------------------
eth-0-1   up        a-full  a-1000  access  1000BASE_T
eth-0-2   admin down auto    auto    access  1000BASE_T
```

2.1.3 Interface Speed Configuration

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# speed 100	Set interface eth-0-1 speed as 100M.
Switch(config-if)# no shutdown	Interface UP
Switch(config-if)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface UP
Switch(config-if)# speed 1000	Set interface eth-0-2 speed as 1000M.
Switch(config-if)# interface eth-0-3	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface UP
Switch(config-if)# speed auto	Set eth-0-3 speed as speed auto mode
Switch(config)# end	Exit exec mode
Switch# show interface status	Show interface status

II. Command validation

Switch# show interface status

```
Port      Status    Duplex  Speed    Mode    Type
-------------------------------------------------------------
eth-0-1   up        a-full  100      access  1000BASE_T
eth-0-2   up        a-full  1000     access  1000BASE_T
eth-0-3   up        a-full  a-1000   access  1000BASE_T
```

2.1.4 Interface Duplex Configuration

There are three situations for setting interface duplex:

- The situation requiring receiving data packets while sending data packets requires interface full-duplex.
- The situation requiring sending or receiving data packets at one time only requires interface half-duplex.
- The situation requiring auto-negotiation about the needed duplex attribute between the home and opposite interfaces requires auto attribute.

Users can choose a duplex mode depending on the actual networking needs.

I. Configuration

Switch# configure terminal	Enter global configuration mode

Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# duplex full	Set interface eth-0-1 as full-duplex.
Switch(config-if)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# duplex half	Set interface eth-0-2 as half-duplex.
Switch(config)# interface eth-0-3	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# duplex auto	Set eth-0-3 speed as duplex auto
Switch(config-if)# end	Exit exec mode.
Switch# show interface status	Show interface status

II. Command validation

Switch# show interface status

```
Port      Status    Duplex  Speed    Mode    Type
-------------------------------------------------------------------
eth-0-1   up        full    a-1000   access  1000BASE_T
eth-0-2   up        half    a-100    access  1000BASE_T
eth-0-3   up        a-full  a-1000   access  1000BASE_T
```

2.2 Layer 3 Interface Configuration

2.2.1 Introduction

The system supports three types of Layer 3 interfaces:

- VLAN interface: You can create any VLAN interface for traffic you want to forward and route.
- Routed port: Switch from physical port to routed port using no switchport.
- Layer 3 link aggregation port: Link aggregation port, made up of routed ports.

Each Layer 3 interface has at least one IP address, and all Layer 3 interfaces require an IP address for routing. This document sets forth how to configure Layer 3 interfaces and how to assign an IP address to an interface.

2.2.2 Configure Routed Port

The steps of configuring routed ports are as below.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no switchport	Set interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable interface
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address 1.1.1.1/24
Switch(config-if)# end	Exit EXEC mode
Switch# show ip interface brief	Show configuration

II. Command validation

Switch# show ip interface brief

```
Interface          IP-Address     Status            Protocol
eth-0-1            1.1.1.1        up                up
Switch# show ip interface
Interface eth-0-1
  Interface current state: UP
  Internet address(es):
    1.1.1.1/24 broadcast 1.1.1.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  VRRP master of:  VRRP is not configured on this interface
```

2.2.3 Configure Routed Port Subinterface

The steps of configuring routed port interfaces are as below.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no switchport	Set interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable interface

Switch(config-if)# subif 5 encapsulation-dot1q 5	Enter subinterface mode
Switch(config-if)# ip address 11.11.11.11/24	Configure subinterface IP address 10.10.10.10/24
Switch(config-subif)# ip address 100.100.10.10/24 secondary	Configure subinterface secondary IP address 100.100.10.10/24
Switch(config-subif)# ip vrf forwarding vpn1	Configure subinterface vrf
Switch(config-subif)# exit-subif	Exit subinterface mode
Switch(config-if)# end	Exit EXEC mode
Switch# show interface eth-0-1 subif 5	Show subinterface

II. Command validation

Switch# show interface eth-0-1 subif 5

```
Interface eth-0-1 subif 5
  Interface current state: UP
  Hardware is Subif, address is d886.0b00.09d5 (bia d886.0b00.09d5)
  Encapsulation-dot1q 5
  Bandwidth 1000000 kbits
  Index 16901 , Metric 1 , Encapsulation ARPA
  The maximum transmit unit (MTU) is 1500 bytes
  VRF binding: associated with vpn1
  VRRP master of :  VRRP is not configured on this interface
  ARP timeout 01:00:00,  ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is disabled
```

Switch# show ip interface brief

```
Interface          IP-Address     Status          Protocol
eth-0-1 subif 5    11.11.11.11    up              up
agg15 subif 15     15.15.15.2     up              up
eth-0-1            unassigned     down            down
eth-0-2            unassigned     down            down
eth-0-3            3.3.3.1        down            down
eth-0-4            unassigned     down            down
eth-0-9            9.9.9.1        down            down
eth-0-14           unassigned     up              up
eth-0-15           unassigned     down            down
eth-0-40           1.1.1.2        down            down
eth-0-48           48.48.48.1     up              up
agg15              unassigned     up              up
vlan1              unassigned     down            down
```

2.2.4 Configure VLAN Interfaces

Multiple virtual VLAN interfaces can be configured on one Ethernet interface. Once being created, any VLAN interface has the functions same as that of physical interface and can be configured and displayed as any physical interface is. VLAN interfaces can be used for dynamic routing protocols such as RIP, OSPE and BGP on the whole network.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN interface configuration mode
Switch(config-vlan)# vlan 10	Create VLAN 10
Switch(config-vlan)# exit	Exit VLAN interface configuration mode
Switch(config)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# switchport mode trunk	Set switchport mode as trunk
Switch(config-if)# switchport trunk allowed vlan all	Add the port into all VLANs
Switch(config-if)# no shutdown	Enable interface
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface vlan10	Enter vlan interface configuration mode
Switch(config-if)# ip address 2.2.2.2/24	Configure IP address 2.2.2.2/24
Switch(config-if)# end	Exit EXEC mode
Switch# show ip interface brief	Show configuration

II. Command validation

Switch# show ip interface brief

Interface	IP-Address	Status	Protocol
vlan10	2.2.2.2	up	up

Switch# show ip interface

```
Interface vlan10
  Interface current state: UP
  Internet address(es):
    2.2.2.2/24 broadcast 2.2.2.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
```

ICMP error messages limited to one every 1000 milliseconds
ICMP redirects are always sent
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are always sent
ARP timeout 01:00:00, ARP retry interval 1s
VRRP master of : VRRP is not configured on this interface

2.3 Interface Errdisable Configuration

2.3.1 Introduction

Errdisable is a system protection mechanism by shutting down abnormal interfaces. There are two ways to recover interfaces in Errdisable state. The first way is to enable Errdisable recovery before Errdisable detection to allow automatic recovery of interfaces after the set time. In the case that Errdisable precedes Errdisable recovery enabling, Errdisable will not automatically recover. The second way is to configure command “no shutdown” on Errdisable interfaces.

Flap suppression of interface link status is an error caused by potential hardware or wiring problems. Admins can also configure the detecting conditions for interface link flap suppression.

2.3.2 Configure Errdisable Detect

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# errdisable detect reason link-flap	Enable link-flap suppression detect errdisable
Switch(config)# end	Exit exec mode
Switch# show errdisable detect	Show errdisable detect

II. Command validation

Switch# show errdisable detect

ErrDisable Reason Detection status
---------- ----------
bpduguard Enabled
bpduloop Enabled
link-monitor-failure Enabled
oam-remote-failure Enabled
port-security Enabled
link-flap Enabled
monitor-link Enabled
udld Enabled
fdb-loop Enabled

```
loopback-detection      Enabled
reload-delay            Enabled
```

2.3.3 Configure Errdisable Recovery

I. Configure

Switch# configure terminal	Enter global configuration mode
Switch(config)# errdisable recovery reason link-flap	Enable erridisable recovery
Switch(config)# errdisable recovery interval 30	Set recovery interval
Switch(config)# end	Exit exec mode
Switch# show errdisable recovery	Show erridisable recovery

II. Command validation

Switch# show errdisable recovery

```
ErrDisable Reason       Timer Status
-----------------       --------------
bpduguard               Disabled
bpduloop                Disabled
link-monitor-failure    Disabled
oam-remote-failure      Disabled
port-security           Disabled
link-flap               Enabled
udld                    Disabled
fdb-loop                Disabled
loopback-detection      Disabled
Timer interval: 30 seconds
```

2.3.4 Configure Errdisable Flap Suppression

Switch# configure terminal	Enter global configuration mode
Switch(config)# errdisable flap reason link-flap 20 60	Set link lap condition 20 times per minute
Switch(config)# end	Exit global configuration mode
Switch# show errdisable flap	Show erridisable flap

```
Switch# show errdisable flap
ErrDisable Reason       Flaps     Time (sec)
-----------------       ------    ----------
link-flap               20        60
```

2.3.5 Configure Disabling Ports from Errdisable Status

Admins can control whether to enter errdisable status or not in the event of mac flap via this command

Switch(config-if)#no errdisable	The port is not entering Errdisable status
Switch(config-if)#errdisable	The port is entering Errdisable status

2.3.6 Check Errdisable Status

Admins can check port errdisable status via two commands, as shown in the commands and configuration instructions in the table below.

Switch# show errdisable recovery	Show erridisable recovery
Switch# show interface status	Show interface status

If errdisable recovery is enabled, the command line will show the time needing to complete recovery; otherwise show not recovered.

Eg.1: Enable link-flap suppression errdisable

```
Switch# show errdisable recovery
ErrDisable Reason       Timer Status
-----------------       --------------
bpduguard               Disabled
bpduloop                Disabled
link-monitor-failure    Disabled
oam-remote-failure      Disabled
port-security           Disabled
link-flap               Enabled
udld                    Disabled
fdb-loop                Disabled
loopback-detection      Disabled
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Interface Errdisable Reason Time Left(sec)
--------- ----------------- --------------
eth-0-3   link-flap         25
```

Eg.2: Disable link-flap suppression errdisable

Switch# show errdisable recovery

```
ErrDisable Reason       Timer Status
-----------------       --------------
```

```
bpduguard               Disabled
bpduloop                Disabled
link-monitor-failure    Disabled
oam-remote-failure      Disabled
port-security           Disabled
link-flap               Disabled
udld                    Disabled
fdb-loop                Disabled
loopback-detection      Disabled
Timer interval: 300 seconds
```

The interface status command also shows a short message indicating interface errdisable status.

Switch# show interface status

```
Port      Status     Duplex   Speed    Mode    Type         Description
--------------------------------------------------------------------------------
eth-0-1   up         a-full   a-1000     TRUNK   1000BASE_SX
eth-0-2   down       auto     auto       TRUNK   Unknown
eth-0-3   errdisable a-full   a-1000   TRUNK   1000BASE_SX
eth-0-4   down       auto     auto       ACCESS  Unknown
```

2.4 MAC Table Configuration

2.4.1 Introduction

MAC address table provides address information for forwarding traffic between switch ports. The address types provided in the table are as follows:

- Dynamic address: Learn from the source address of switches, and go into aging status if learning failed after the aging time. We support IVL learning mode only.
- Static address: Source addresses manually added by admins.

2.4.2 References

IEEE 802.1D

IEEE 802.1Q

2.4.3 Terms

The below describes terms and concepts involved in the MAC address table.

IVL: Independent VLAN learning: For a given VLAN, a specific MAC address that is learning in one VLAN cannot be taken as the forwarding decision of any other VLAN.

SVL: Sharing VLAN learning: For a given VLAN, a specific MAC address that is learning in one VLAN can be taken as the forwarding decision of any other VLAN.

2.4.4 Address Ageing Time Configuration

Ageing time is not an exact time. If the ageing time is set as N, the dynamic address will age after an interval N - 2N. The default ageing time is 300 seconds.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# mac-address-table ageing-time 10	Set dynamic address ageing time as 10 seconds.
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table ageing-time	Show address ageing time

II. Command validation

Switch# show mac address-table ageing-time

MAC address table ageing time is 10 seconds

2.4.5 Static Unicast Address Configuration

Unicast address table can be associated with one port only.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# mac-address-table 0000.1234.5678 forward eth-0-1 vlan 1	Add static unicast address
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table	Show MAC address table

II. Command validation

Switch# show mac address-table

Mac Address Table

(*) - Security Entry

Vlan	Mac Address	Type	Ports
1	0000.1234.5678	static	eth-0-1

2.4.6 Static Multicast Address Configuration

Multicast addresses can be associated with multiple ports.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-1 vlan 1	Add static multicast addresses to interface eth-0-1
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-2 vlan 1	Add static multicast addresses to interface eth-0-2
Switch(config)# end	Exit to EXEC mode
Switch# show mac address-table	Show MAC address table

II. Command validation

Switch# show mac address-table

```
  Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan    Mac Address      Type      Ports
----   --------------   -------    -------
1      0100.0000.0000   static     eth-0-1
                                   eth-0-2
```

2.4.7 MAC Address Filtering Configuration

MAC filtering will discard those source or destination addresses set as discard data frame. The priority of AC filtering is higher than that of MAC addresses.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# mac-address-table 0000.1234.5678 discard	Add unicast addresses to discard
Switch(config)# end	Exit to EXEC mode
Switch# show mac-filter address-table	Show MAC address table

II. Command validation

Switch# show mac-filter address-table

```
   MAC Filter Address Table
---------------------------------
```

```
Current count     : 0
Max count         : 128
Left count        : 128
Filter address list :
-----------------------------------
```

2.5 VLAN Configuration

2.5.1 Introduction

VLAN (Virtual Local Area Network) is a network logically divided into different broadcast domains, so as to swap data packet between ports in the same VLAN only. Every VLAN is regarded as a logic network, so data packets not belonging to the same VLAN must be forwarded by routing.

2.5.2 Configure Access Port

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 2	Create VLAN 2
Switch(config-vlan)# exit	Exit VLAN mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport mode access	Set interface type as access
Switch(config-if)# switchport access vlan 2	Specify port to corresponding VLAN
Switch(config-if)# end	Exit configuration mode
Switch# show vlan brief	Show VLAN configuration brief
Switch# show interface switchport interface eth-0-1	Show switch interface information

II. Command validation

```
Switch# show interface switchport interface eth-0-1
 Interface name            : eth-0-1
 Switchport mode           : access
 Ingress filter            : enable
 Acceptable frame types    : vlan-untagged only
 Default Vlan              : 2
 Configured Vlans          :   2
Switch# show vlan brief
VLAN ID  Name          State   STP ID      Member ports
```

```
                                    (u)-Untagged, (t)-Tagged
======= ================ ======= =======  ========================
1       default          ACTIVE  0       eth-0-2(u) eth-0-3(u)
                                         eth-0-4(u) eth-0-5(u)
                                         eth-0-6(u) eth-0-7(u)
                                         eth-0-8(u) eth-0-9(u)
                                         eth-0-10(u) eth-0-11(u)
                                         eth-0-12(u) eth-0-13(u)
                                         eth-0-14(u) eth-0-15(u)
                                         eth-0-16(u) eth-0-17(u)
                                         eth-0-18(u) eth-0-19(u)
                                         eth-0-20(u) eth-0-21(u)
                                         eth-0-22(u) eth-0-23(u)
2       VLAN0002         ACTIVE  0       eth-0-1(u)
```

2.5.3 Trunk Port Configuration

Trunk ports can receive tagged, untagged and priority-tagged frames and send untagged and tagged frames. If a port receives an untagged frame, the frame will assign the port's PVID as VLAN ID; if a frame's VID is equal to the port's PVID, the frame will peel off the VLAN tag when being sent.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 10,20	Create VLAN 10, 20
Switch(config-vlan)# exit	Exit VLAN mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport mode trunk	Set port as trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set port to allow VLAN all
Switch(config-if)# switchport trunk native vlan 10	Set native port VLAN as 10
Switch(config-if)# exit	Exit interface mode

II. Command validation

Switch# show interface switchport

```
Interface name          : eth-0-1
Switchport mode         : trunk
Ingress filter          : enable
Acceptable frame types  : all
Default Vlan            : 10
Configured Vlans        :   1   10   20
```

```
Interface name            : eth-0-2
Switchport mode           : access
Ingress filter            : enable
Acceptable frame types  : vlan-untagged only
Default Vlan              : 10
Configured Vlans          :   10
Switch# show vlan brief
VLAN ID  Name          State   STP ID      Member ports
                                  (u)-Untagged, (t)-Tagged
======= ================ ======= =======  ========================
1      default         ACTIVE  0       eth-0-1(t) eth-0-3(u)
                                       eth-0-4(u) eth-0-5(u)
                                       eth-0-6(u) eth-0-7(u)
                                       eth-0-8(u) eth-0-9(u)
                                       eth-0-10(u) eth-0-11(u)
                                       eth-0-12(u) eth-0-13(u)
                                       eth-0-14(u) eth-0-15(u)
                                       eth-0-16(u) eth-0-17(u)
                                       eth-0-18(u) eth-0-19(u)
                                       eth-0-20(u) eth-0-21(u)
                                       eth-0-22(u) eth-0-23(u)
10     VLAN0010        ACTIVE  0       eth-0-1(t) eth-0-2(u)
20     VLAN0020        ACTIVE  0       eth-0-1(t)
```

2.6 VOICE VLAN Configuration

2.6.1 Introduction

With the increasing development of voice technology, IP phones and IAD (Integrated Access Device) are more and more widely used. Especially in broad-band resident district, it is common that voice data and business data coexist in the network. Voice data transmission requires a higher superiority than business data to reduce possible time delay and packet dropout in transmission.

The conventional method of raising the superiority of voice data transmission is to differentiate voice data using ACL and utilize QoS for transmission quality guarantee. To simplify user configuration and facilitate management of transmission policy of voice traffic, device machines are provided with Voice VLAN feature. Voice VLAN is mainly characterized by the ability of automatically recognizing voice traffic based on the source MAC addresses in messages to guarantee voice traffic transmission.

2.6.2 Configure VOICE VLAN

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 2	Create VLAN2
Switch(config-vlan)# exit	Exit VLAN mode,

Switch(config)# voice vlan 2	Assign VLAN as VOICE VLAN
Switch(config)# voice vlan mac-address 0055.0000.0000 ffff.ff00.0000 description test	Add an entry to appoint a type of MAC as VOICE VLAN
Switch(config)# interface eth-0-1	Enter interface eth-0-1 configuration mode
Switch(config-if)# switchport mode trunk	Set port as trunk port
Switch(config-if)# switchport trunk allowed vlan all	Allow all tagged VLANs through the port
Switch(config-if)# voice vlan enable	Enable VOICE VLAN on port
Switch(config-if)# interface eth-0-2	Enter interface eth-0-2 configuration mode
Switch(config-if)# switchport mode trunk	Set port as trunk port
Switch(config-if)# switchport trunk allowed vlan all	Allow all tagged VLANs through the port

2.6.3 Command Validation

Send messages to eth-0-1 in the following format:

```
0x0000:  0000 0a02 0001 0055 0000 0011 8100 0002  ........k.......
0x0010:  0800 aadd aadd aadd aadd aadd aadd aadd  ................
0x0020:  aadd aadd aadd aadd aadd aadd aadd aadd  ................
0x0030:  aadd aadd aadd aadd aadd aadd            ............
```

The priority of Vlan tag field is 0

Receive messages via eth-0-2 in the following format:

```
0x0000:  0000 0a02 0001 0055 0000 0011 8100 a002  ........k.......
0x0010:  0800 aadd aadd aadd aadd aadd aadd aadd  ................
0x0020:  aadd aadd aadd aadd aadd aadd aadd aadd  ................
0x0030:  aadd aadd aadd aadd aadd aadd            ............
```

After calculation, it can be seen that the priority of vlan tag field has been changed to 5.

2.7 VLAN Classification Configuration

2.7.1 Overview

VLAN classification is to send data packets to selected VLAN as per the detailed rules of protocols or subnet standards. A type of rule set can be applied to one interface.

There are three types of VLAN classification rules: MAC-based, IP-based and protocol-based. MAC-based VLAN classification rule is to classify data packets based on their source MAC address; IP-based VLAN classification rule refers to classification based on the source IP

address of data packets; protocol-based VLAN classification rule refers to classification based on the Layer 3 protocol type of data packets. The Layer 3 types below supports ARP, IP (V4), MPLS, MCAST MPLS, PPPoE protocol and RARP.

VLAN classification rules of different types can be added to a same VLAN type group. Only one VLAN classification rule can be activated on one switch port.

2.7.2 Topology

In the configuration example below, the three VLAN classification rules are created:

- The first is MAC-based rule in which source MAC 2222.2222.2222 is classified into VLAN 5;
- The second is IP-based rule in which source IP 1.1.1.1 is classified into VLAN 5;
- The third is protocol-based rule in which ARP protocol data unit is classified into VLAN 5.

Add rules 1, 2 and 3 into Group 31, and apply Group 31 to the three interfaces. Apply respective classification strategies to interfaces eth-0-1, eth-0-2 and eth-0-3. Eth-0-1 is IP-based classification, meaning the data packets matching the IP will be forwarded from the port to the corresponding VLAN by rule. Eth-0-2 is MAC-based classification, meaning the data packets matching the MAC address will be forwarded to the corresponding VLAN by rule. Eth-0-3 is protocol-based classification, meaning the data packets matching the protocol will be forwarded to the corresponding VLAN by rule.

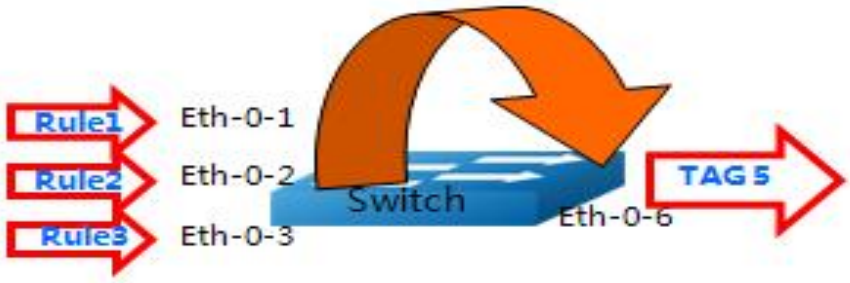


Figure 2-1 Topological Graph of VLAN Classification

2.7.3 Configuration

VLAN Classification Configuration Details

Run command “show vlan classifier group” to show all VLAN classification groups; run command “show vlan classifier rule” to show all VLAN classification rules.

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 5	Create VLAN5
Switch(config-vlan)# vlan 6	Create VLAN6
Switch(config-vlan)# exit	Exit VLAN mode

Switch(config)# vlan classifier rule 1 mac 2222.2222.2222 vlan 5	Create MAC-based VLAN classification rule
Switch(config)# vlan classifier rule 2 ip 1.1.1.1 vlan 5	Create IP-based VLAN classification rule
Switch(config)# vlan classifier rule 3 protocol arp vlan 5	Create protocol-based VLAN classification rule
Switch(config)# vlan classifier group 31 add rule 1	Add Rule 1 into Group 31
Switch(config)# vlan classifier group 31 add rule 2	Add Rule 2 into Group 31
Switch(config)# vlan classifier group 31 add rule 3	Add Rule 3 into Group 31

Interface Configuration Details

Run command “show vlan classifier interface group” to show interface VLAN classification information.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID 6 to eth-0-1
Switch(config-if)# switchport access allowed vlan add 5	Interface allows VLAN5
Switch(config-if)# vlan classifier activate 31 based ip	Apply Group 31 to the interface and set interface VLAN classification as IP-based type
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID 6 to eth-0-2
Switch(config-if)# switchport access allowed vlan add 5	Interface allows VLAN5
Switch(config-if)# vlan classifier activate 31 based mac	Apply Group 31 to the interface and set interface VLAN classification as MAC-based type
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-3	Enter interface mode
Switch(config-if)# switchport access vlan 6	Assign PVID 6 to eth-0-3
Switch(config-if)# switchport access allowed vlan add 5	Interface allows VLAN5

Switch(config-if)# vlan classifier activate 31 based protocol	Apply Group 31 to the interface and set interface VLAN classification as protocol-based type
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-6	Enter interface mode
Switch(config)#switchport mode trunk	Configure the port as trunk mode
Switch(config-if)# switchport trunk allowed vlan add 5	Add eth-0-6 into VLAN5
Switch(config-if)# exit	Exit interface mode

2.7.4 Command Validation

Step 1 Verify VLAN classification rules.

Switch# show vlan classifier rule

vlan classifier rule 1 mac 2222.2222.2222 vlan 5
vlan classifier rule 2 ip 1.1.1.1 vlan 5
vlan classifier rule 3 protocol arp vlan 5

Step 2 Verify VLAN classification groups.

Switch# show vlan classifier group

vlan classifier group 31 add rule 1
vlan classifier group 31 add rule 2
vlan classifier group 31 add rule 3

Step 3 Verify VLAN classification rule interface application.

Switch# show vlan classifier interface grou

vlan classifier group 31 on interface eth-0-2, based mac
vlan classifier group 31 on interface eth-0-1, based ip
vlan classifier group 31 on interface eth-0-3, based protocol

2.8 VLAN Mapping Configuration

2.8.1 Configure VLAN Translation

I. Overview

Service vendor's service subscribers usually requires specific VLAN ID. The VLANs required by customers of the same vendor may coincide, and user traffic flowing through the vendor's devices may be mixed. The communications of customers of different applications can be differentiated by mapping the VLAN ID assigning a unique VLAN ID to each customer.

VLAN translation feature facilitates vendors serving customers in possession of their own VLAN ID with a series VLANs. By translating customer VLAN ID, the traffic from customers of different applications is differentiated on the vendor's devices even in the same VLAN.

II. Topology

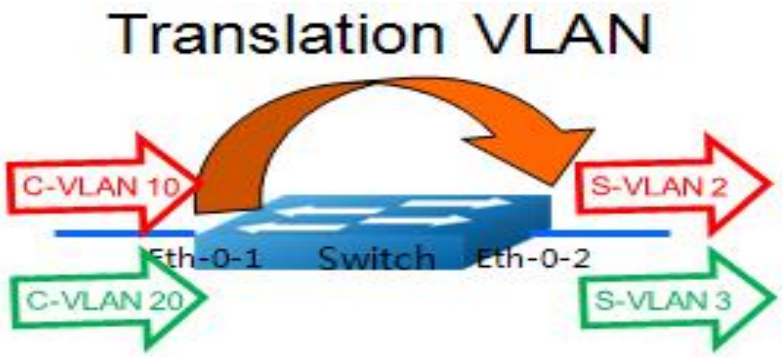


Figure 2-2 Topological Graph of VLAN Translation

III. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 2,3	Create S-TAG VLAN 2,3
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set VLAN2 to be associated with EVE evc_c1
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set VLAN2 to be associated with EVE evc_c2
Switch(config)# vlan mapping table vm	Create VLAN MAPPING table VM
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Set C-Tag as 10 and as 2 by mapping to S-Tag
Switch(config-vlan-mapping)# raw-vlan 20 evc evc_c2	Set C-Tag as 20 and as 3 by mapping to S-Tag
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport mode trunk	Configure the port as trunk mode

Switch(config-if)# switchport trunk vlan-translation	Set trunk as VLAN translation mode
Switch(config-if)# switchport trunk vlan-translation mapping table vm	Apply VLAN mapping table to the interface
Switch(config-if)# switchport trunk allowed vlan add 2,3	Add VLAN 2, 3
Switch(config-if)# interface eth-0-2	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the port as trunk mode
Switch(config-if)# switchport trunk allowed vlan add 2,3	Add VLAN 2, 3
Switch(config-if)# end	Exit interface mode
Switch# show interface switchport interface eth-0-1	Check port configuration
Switch# show vlan mapping table	Check Vlan mapping table

IV. Command validation

Switch# show interface switchport interface eth-0-1

```
Interface name              : eth-0-1
 Switchport mode            : trunk
 VLAN traslation            : enable
 VLAN mapping table         : vm
 Ingress filter             : enable
 Acceptable frame types     : all
 Default Vlan               : 1
 Configured Vlans           : 1    2    3
Switch# show vlan mapping table
Table Name       EVC Name         Mapped VLAN Raw VLAN
 ================ ================ =========== ======================
vm               evc_c1           2           10
                 evc_c2           3           20
```

2.8.2 Configure 802. 1Q Tunneling

I. Introduction

QinQ technology has largely expanded the count of VLAN to as many as 4096 × 4096 by stacking two 802.1Q packet headers in Ethernet frame. Meanwhile, multiple VLANs can be reused in a core VLAN. ISP usually builds one VLAN model for each customer, utilizes GARP/GVRP to automatically monitor the VLAN of the entire backbone network, and accelerates network convergence by extending STP, so as to make the network of resilience.

QinQ technology is a good choice as an initial solution, but SVLAN model also will bring about scalability problem with the increase of users. Since some users may want to transmit data with their own VLAN ID between branches, the MSP equipped with QinQ technology will encounter two problems. The first customer's VLAN ID may conflict with other customers'. The service providers may be severely limited the count of customer's available identifiers. If users are allowed to use their respective VLAND ID space in their own way, the core network is still limited by 4096 VLANs.

QinQ refers to encapsulating users' private VLAN tag in public VLAN tag to enable messages to flow through operators' backbone network (public network) with VLAN tags of two layers. In the public network, messages are spread based on the outer layer VLAN tag (namely public VLAN tag) only, and users' private VLAN tags are screened. In this way, data flows are differentiated, and users' VLAN tags can be reused due to transparent transfer of private VLAN tags with outer VLAN tag being unique in the public network, which actually increases the number of available VLAN tags.

There are two methods of encapsulating outer VLAN tags. The first one is standard QINQ encapsulation, namely port-based tagging outside. All user data under the port is encapsulated in a shared VLAN tag. It has great limitation in practical use. The other one is flexible QINQ encapsulation, with which flow classification of user data can be made by some features, and different outer VLAN tags are encapsulated in different types.

II. Configure standard QINQ

Topology

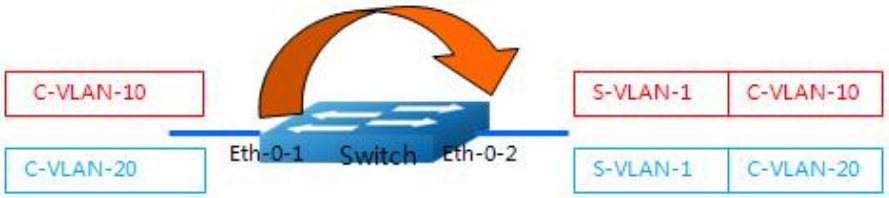


Figure 2-3 Basic 802.1Q tunneling topological graph

Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode dot1q-tunnel	Configure the interface as DOT1Q-Tunnel mode
Switch(config-if)# end	Exit interface mode
Switch# show interface switchport interface eth-0-1	Check interface configuration

Command Validation

This example shows how to configure switch ports of a basic 802.1q tunnel portal. Run command "show" to show interface configuration.

Switch# show interface switchport interface eth-0-1

```
Interface name          : eth-0-1
 Switchport mode        : dot1q-tunnel(basic)
 Ingress filter         : enable
 Acceptable frame types : all
 Default Vlan           : 1
 Configured Vlans       : 1
```

III.Configure flexible QINQ

The steps of configuring U-tag messages plus a layer of tag are as below.

Topology

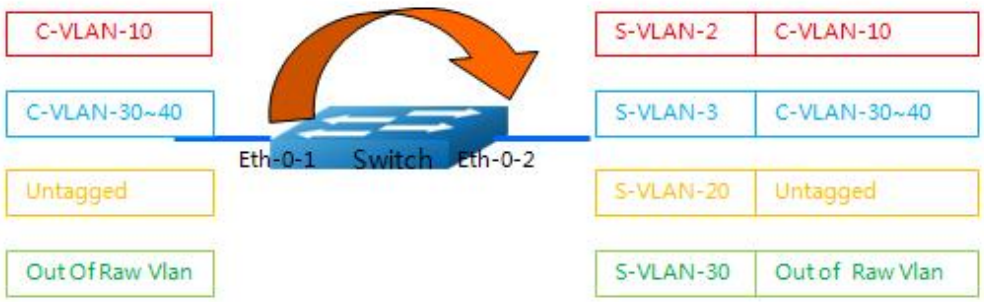


Figure 2-4 Add a layer of tag

Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 2,3,20,30	Create S-TAG 2, 3, 20, 30
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set S-TAG 2 to be associated with EVC_C1
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set S-TAG 3 to be associated with EVC_C2

Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 20	Set S-TAG 20 to be associated with EVC_C3
Switch(config)# ethernet evc evc_c4	Create EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 30	Set S-TAG 30 to be associated with EVC_C4
Switch(config)# vlan mapping table vm	Create Vlan mapping table
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Add C-TAG10 into evc_c1
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	Add C-TAG30-40 into evc_c2
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	Add U-TAG into evc_c3
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	Add out-of-range C-TAG into evc_c4
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport mode dot1q-tunnel	Set the interface as Dot1q-tunnel mode
Switch(config-if)# switchport dot1q-tunnel type selective	Set the interface as flexible QINQ
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	Apply VLAN mapping table VM to the interface
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	The interface allows VLAN 2, 3, 20, 30
Switch(config-if)# interface eth-0-2	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk mode
Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	The interface allows VLAN 2, 3, 20, 30
Switch(config-if)# end	Exit interface mode
Switch# show interface switchport interface eth-0-1	Check port configuration
Switch# show vlan mapping table	Check VLAN mapping table

Command Validation

This example shows how to configure a flexible QINQ. Run command "show" to show interface configuration.

Note: If eth-0-1 tpid differs from eth-0-2 tpid, users must globally enable qos and set eth-0-2 as replace cos to replace the tpid of the stag from eth-0-2.

Switch# show interface switchport interface eth-0-1

```
Interface name              : eth-0-1
Switchport mode             : dot1q-tunnel(selective)
VLAN mapping table          : vm
Ingress filter              : enable
Acceptable frame types      : all
Default Vlan                : 1
Configured Vlans            : 1   2   3   20   30
Switch# show vlan mapping table
Table Name       EVC Name        Mapped VLAN Raw VLAN
=================================================================
vm               evc_c1          2           10
                 evc_c2          3           30-40
                 evc_c3          20          untagged
                 evc_c4          30          out-of-range
```

The steps of configuring U-tag messages plus two layers of tags are as below.

Topology

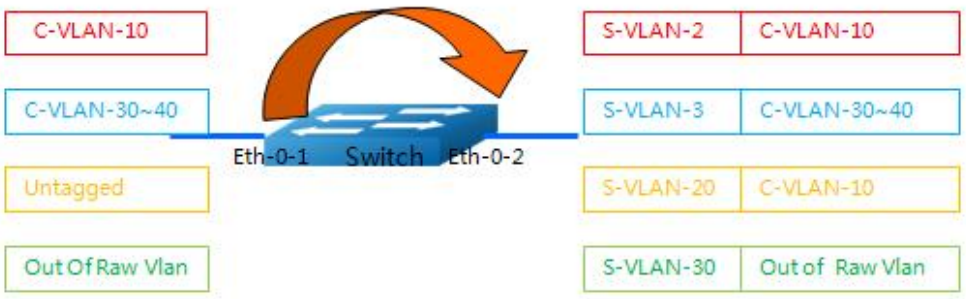


Figure 2-5 Add two layers of tag

Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 2,3,10,20,30	Create S-TAG 2, 3, 10, 20, 30
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Set S-TAG 2 to be associated with evc_c1

Switch(config-evc)# exit	Exit EVC mode
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Set S-TAG 3 to be associated with evc_c2
Switch(config-evc)# exit	Exit EVC mode
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-double-vlan 10 20	Set S-TAG 10 and S-TAG 20 to be associated with evc_c3
Switch(config-evc)# exit	Exit EVC mode
Switch(config)# ethernet evc evc_c4	Created EVC
Switch(config-evc)# dot1q mapped-vlan 30	Set S-TAG 30 to be associated with evc_c4
Switch(config-evc)# exit	Exit EVC mode
Switch(config)# vlan mapping table vm	Create VLAN mapping table
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	Add C-TAG10 into evc_c1
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	Add C-TAG30-40into evc_c2
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	Add U-TAG into evc_c3
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	Add out-of-range C-TAG into evc_c4
Switch(config-vlan-mapping)# exit	Exit mapping configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport mode dot1q-tunnel	Configure the interface as do1q-tunnel
Switch(config-if)# switchport dot1q-tunnel type selective	Set the interface as flexible QINQ
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	Apply VLAN mapping table VM to the interface

Switch(config-if)# switchport dot1q-tunnel native inner-vlan 10	Configure native inner-vlan 10
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	The interface allows VLAN 2, 3, 20, 30
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk mode
Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	The interface allows VLAN 2, 3, 20, 30
Switch(config-if)# end	Exit interface mode
Switch# show interface switchport interface eth-0-1	Check configuration
Switch# show vlan mapping table	Check vlan mapping table entries

Command Validation

This example shows how to configure a flexible QINQ. Use command "show" to show interface configuration.

Switch# show interface switchport interface eth-0-1

```
Interface name              : eth-0-1
Switchport mode             : dot1q-tunnel(selective)
VLAN mapping table          : vm
Ingress filter              : enable
Acceptable frame types      : all
Default Vlan                : 10
Configured Vlans            : 1    2    3    20   30
Switch# show vlan mapping table
Table Name       EVC Name        Mapped VLAN Raw VLAN
================ =============== =========== ==============================
vm               evc_c1          2           10
                 evc_c2          3           30-40
                 evc_c3          20(10)      untagged
                 evc_c4          30          out-of-range
```

2.9 Link Aggregation Configuration

2.9.1 Introduction

This chapter presents an example of link aggregation control protocol (LACP) configuration. LACP protocol is an 802.3ad-based IEEE standard. It allows bundling multiple physical interfaces to form a single logical channel to provide enhanced performance and redundancy. Aggregation port is connected to every switch as a single link. It is regarded as one port in spanning tree. In the event that one physical interface breaks down and other interfaces work normally, the link will not be interrupted. This implementation supports up to 16 physical Ethernet links in a single logical channel. LACP protocol allows our devices to manage link aggregation group between other devices complying with 802.3ad protocol. With LACP protocol, switch learning supports the ability of LACP members of recognizing each port. Then, the dynamic group ports with the same attributes are bound to a single logical link.

2.9.2 References

LACP is based on IEEE 802.3ad standard protocol

2.9.3 Configure Dynamic AGG

I. Topology

For purpose of this example, three links are configured between switches S1 and S2. The three links are assigned into a same management center (1), so that they can aggregate to form a single channel 1.

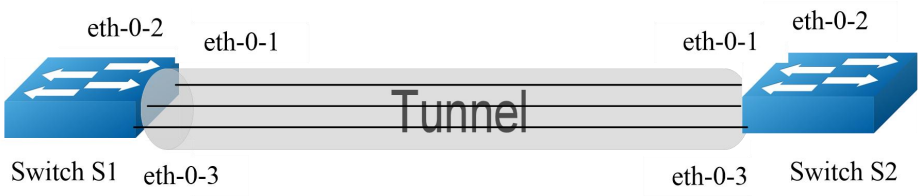


Figure 2-6 LACP Topology

II. Configuration

Switch 1

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# lacp system-priority 2000	Set system priority on this switch. The priority is for deciding the system to resolve conflicts while aggregation group selection. Low numerical value means high priority
Switch1(config)# port-channel load-balance hash-field-select macsa	Realize load balancing via source MAC address

Switch1(config)# interface eth-0-1	Enter interface configuration mode
Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation, so that aggregation selection can be realized in local system
Switch1(config-if)# exit	Exit interface configuration mode
Switch1(config)# interface eth-0-2	Enter interface configuration mode
Switch1(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation in active mode, so that aggregation selection can be realized in local system
Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# exit	Exit interface configuration mode
Switch1(config)# interface eth-0-3	Enter interface configuration mode
Switch1(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation, so that aggregation selection can be realized in local system
Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# end	Exit interface configuration mode

Switch 2

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# lacp system-priority 1000	Set system priority of switch, which is for deciding the system to resolve conflicts while aggregation group selection. Low numerical value means high priority
Switch2(config)# interface eth-0-1	Enter interface configuration mode
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation in active mode, so that aggregation selection can be realized in local system

Switch2(config-if)# exit	Exit interface configuration mode
Switch2(config)# interface eth-0-2	Enter interface configuration mode
Switch2(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation, so that aggregation selection can be realized in local system
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# exit	Exit interface configuration mode
Switch2(config)# interface eth-0-3	Enter interface configuration mode
Switch2(config-if)# channel-group 1 mode active	Add the interface to channel group 1 to enable link aggregation in active mode, so that aggregation selection can be realized in local system
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# end	Exit interface configuration mode

III.Command validation

Switch1# show channel-group summary

```
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
    macsa
Flags:  s - suspend                T - standby
        D - down/admin down   B - in Bundle
        R - Layer3                 S - Layer2
        w - wait                   U - in use
Mode:   SLB  - static load balance
         DLB  - dynamic load balance
         SHLB - self-healing load balance
         RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
----------------+---------+------------+-----------------------------------------------
agg1(SU)        SLB       LACP         eth-0-1(B) eth-0-2(B) eth-0-3(B)
Switch1# show interface agg1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia cce3.33fc.330b)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
```

No virtual circuit configured
ARP timeout 01:00:00, ARP retry interval 1s
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 2 bits/sec, 0 packets/sec
13 packets input, 1184 bytes
Received 0 unicast, 0 broadcast, 0 multicast
0 runts, 0 giants, 0 input errors, 0 CRC
0 frame, 0 overrun, 0 pause input
0 input packets with dribble condition detected
20 packets output, 2526 bytes
Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output

2.9.4 Configure Static AGG

I. Topology

For purpose of this example, three links are configured between switches S1 and S2. The three links are assigned into a same management center (1), so that they can aggregate to form a single channel 1.

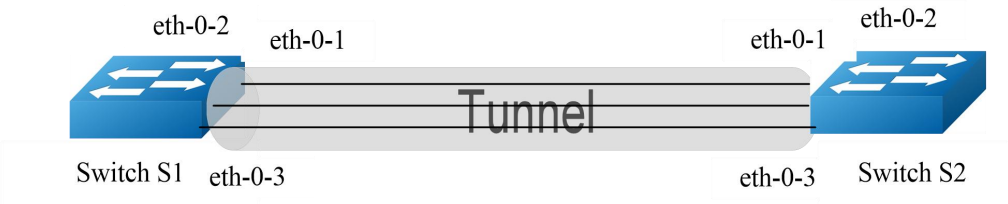


Figure 2-7 LACP Topology

II. Configuration

Switch 1

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# interface eth-0-1	Enter interface configuration mode
Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# static-channel-group 1	Add the interface into channel group 1
Switch1(config-if)# exit	Exit interface configuration mode
Switch1(config)# interface eth-0-2	Enter interface configuration mode
Switch1(config-if)# static-channel-group 1	Add the interface into channel group 1

Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# exit	Exit interface configuration mode
Switch1(config)# interface eth-0-3	Enter interface configuration mode
Switch1(config-if)# static-channel-group 1	Add the interface into channel group 1
Switch1(config-if)# no shutdown	Interface up
Switch1(config-if)# end	Exit interface configuration mode

Switch 2

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-1	Enter interface configuration mode
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# static-channel-group 1	Add the interface into channel group 1
Switch2(config-if)# exit	Exit interface configuration mode
Switch2(config)# interface eth-0-2	Enter interface configuration mode
Switch2(config-if)# static-channel-group 1	Add the interface into channel group 1
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# exit	Exit interface configuration mode
Switch2(config)# interface eth-0-3	Enter interface configuration mode
Switch2(config-if)# static-channel-group 1	Add the interface into channel group 1
Switch2(config-if)# no shutdown	Interface up
Switch2(config-if)# end	Exit interface configuration mode

III. Command validation

Switch1# show channel-group summary

```
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
    macsa
Flags:  s - suspend              T - standby
       D - down/admin down   B - in Bundle
       R - Layer3                S - Layer2
       w - wait                    U - in use
Mode:   SLB  - static load balance
           DLB  - dynamic load balance
           SHLB - self-healing load balance
           RR   - round robin load balance
Aggregator Name  Mode      Protocol     Ports
----------------+---------+------------+-----------------------------------------------
agg1(SU)        SLB       Static       eth-0-1(B) eth-0-2(B) eth-0-3(B)
Switch1# show interface agg 1
Interface agg1
  Interface current state: UP
  Hardware is AGGREGATE, address is cce3.33fc.330b (bia a876.6b2c.9c01)
  Bandwidth 3000000 kbits
  Index 1025 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full  , Media type is Aggregation
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00,  ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 140 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    1080 packets output, 60614 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

2.10 Flow Control Configuration

2.10.1 Introduction

Flow control is enabled on the direct connected Ethernet port, and flow rate is controlled by allowing the congested node on the opposite end to pause link operation during congestion. If the native device detects any congestion locally, it can notify link partners or remote devices of the congestion by sending a pause frame. Immediately after receiving the pause frame, remote devices will stop sending any data packet to avoid discarding any data packet during congestion. For auto-negotiation link, the local flow controllability can be notified to the opposite side via link disconnection/connection.

2.10.2 Topology

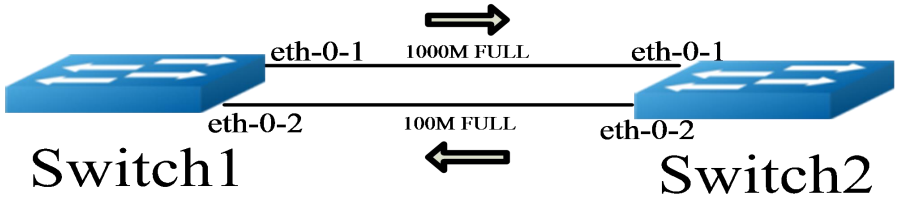


Figure 2-8 Flow control

2.10.3 Configure Sending Flow Control Messages

Switch2# configure terminal	Enter configuration mode
Switch2(config)# interface eth-0-1	Enter interface mode
Switch2(config-if)# flowcontrol send on	Enable flow control message sending on the interface
Switch2(config-if)# exit	Go back to configuration mode

NOTE

Flow control is valid on full-duplex links only

2.10.4 Configure Receiving Flow Control Messages

Switch1# configure terminal	Enter configuration mode
Switch1(config)# interface eth-0-1	Enter interface mode
Switch1(config-if)# flowcontrol receive on	Enable flow control message receiving on the interface
Switch1(config-if)# exit	Go back to configuration mode

2.10.5 Configuration Verification

Switch2# show flowcontrol

```
Port      Receive FlowControl  Send FlowControl  RxPause     TxPause
          admin    oper        admin    oper
--------- -------- --------    -------- --------  ----------- -----------
eth-0-1   off      off         on       on        0           0
eth-0-2   off      off         off      off       0           0
eth-0-3   off      off         off      off       0           0
```

Switch2# show flowcontrol eth-0-1

```
Port      Receive FlowControl  Send FlowControl  RxPause     TxPause
```

```
          admin    oper       admin    oper
---------  -------- --------   -------- --------  -----------  -----------
eth-0-1    off      off        on       on        0            0
```

Switch1# show flowcontrol

```
Port      Receive FlowControl  Send FlowControl   RxPause      TxPause
          admin    oper        admin    oper
---------  -------- --------   -------- --------  -----------  -----------
eth-0-1    on       on          off      off      0            0
eth-0-2    off      off         off      off      0            0
eth-0-3    off      off         off      off      0            0
```

Switch1# show flowcontrol eth-0-1

```
Port      Receive FlowControl  Send FlowControl   RxPause      TxPause
          admin    oper        admin    oper
---------  -------- --------   -------- --------  -----------  -----------
eth-0-1    on       on          off      off      0            0
```

2.11 Loopback Detection Configuration

2.11.1 Introduction

Network loops will lead to repeated send of broadcast, multicast and unknown unicast messages, causing the waste of network resources and even network paralysis. To detect loops in Layer 2 network in time to avoid serious impacts on the whole network, a detection function is needed, so that users can be promptly reminded to check network connection and configurations in the case of network loops and the interfaces going wrong can be put under control.

Loopback detection function is for detecting device interface loopback. It sends a detection message through the interface regularly and detects whether the message is received via the interface of sending. If the interface receives the detection message, it is regarded that loops have been formed in this interface. Then, warning messages can be sent to the network management system promptly to remind the admins of and to eliminate network loops, so as to avoid long-time network traffic anomaly. Additionally, it is workable to put device interface under control, and configure Trap or shutting down the interface as needed to minimize the impact of loopback on the network.

2.11.2 Configure Enabling Loopback Detect

By default, the loopback detection function is disabled, and the interface will send loopback detect messages for interface loopback detect only after the loopback detection function of the interface is enabled. The default interval of sending detect messages is 5 seconds.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode

Switch(config-if)# loopback-detect enable	Enable Loopback Detect.
Switch(config)#end	Exit configuration mode
Switch#show loopback-detect	Show loopback detect status

II. Command validation

```
Switch# show loopback-detect
Loopback detection packet interval(second): 5
Loopback detection recovery time(second):   15
Interface       Action          Status
eth-0-2         shutdown        NORMAL
```

2.11.3 Configure Interval of Sending Loopback Detect Messages

Since the network keeps changing, loopback detect is a continuing process. The interface sends loopback detect messages at a certain interval, which is called interval of loopback detection message sending.

I. Configuration

The system supports configuring the interval of sending loopback detection messages (1-300 seconds). The time needed for loopback status recovery is triple of the sending interval and is not less than 10 seconds. The interface status will be restored as before after loops are eliminated.

Switch#configure terminal	Enter configuration mode
Switch(config)# loopback-detect packet-interval 10	Set the sending interval of loopback detect messages as 10 seconds
Switch(config-if)# end	Exit configuration mode
Switch# show loopback-detect packet-interval	Validate the sending interval command of loopback detect messages

II. Command validation

```
Switch# show loopback-detect packet-interval
Loopback detection packet interval(second): 10
Loopback detection recovery time(second):   30
```

2.11.4 Configure Loopback Detect Processing Action

If interface loopback is detected, the device will set the interface into loopback detection state, and such processing actions

as sending warnings and shutting down interface can be configured.

I. Configuration

Once the loopback detection function is enabled, the interface will detect whether loopback messages are received periodically. Users can

configure the mode of processing in the case that loopback messages are detected to reduce the impact of loops on this device and the whole network as far as possible.

Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# loopback-detect action shutdown	Configure loopback detect processing action as shutdown
Switch(config-if)# end	Exit configuration mode
Switch# show loopback-detect interface eth-0-1	Validate command

II. Command validation

```
Switch# show loopback-detect interface eth-0-1
Interface       Action          Status
eth-0-1         shutdown        NORMAL
```

2.11.5 Configure Loopback Detection Function Specific to Designated VLAN

Once the loopback detection function is enabled, the system sends Untag detection messages by default, namely

performing loopback detection on no designated VLAN. If an interface joins VLAN in tagged form, the Untag detection messages from the interface

will be discarded on the link, and the interface will not receive looped back messages, so it is needed to configure loopback detection on specific VLAN. Once the loopback detection function of the designated VLAN is configured, the interface will send an untagged detection message and several detection messages tagged with the designated VLAN regularly, and one interface can send up to 8 detection messages tagged with the designated VLAN.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# loopback-detect packet vlan 20	Configure loopback detect function of VLAN 20 under the interface
Switch(config-if)# end	Exit configuration mode
Switch# show running-config interface eth-0-1	Validate command.

II. Command validation

```
Switch# show running-config interface eth-0-1
```

```
Building configuration...
!
interface eth-0-1
 loopback-detect enable
loopback-detect packet vlan 2
```

2.12 Priority-based Flow Control Configuration

2.12.1 Introduction

Priority-based flow control (PFC) is an enhancement of flow control mechanism (as shown in Figure. 2-1). Currently, zero packet dropout can be realized via Ethernet pause (IEEE 802.3 Annex 31B), but it will block all flows on a link and pause the whole link essentially. PFC allows to create 8 virtual channels on an Ethernet link and assigns an IEEE 802.1P priority for each virtual channel, allows to separately pause or reboot any virtual channel, and allows uninterrupted passage of flows from other virtual channels. By this method, the network can create zero packet dropout services for single virtual link and make it coexist with other flow types on the same interface.

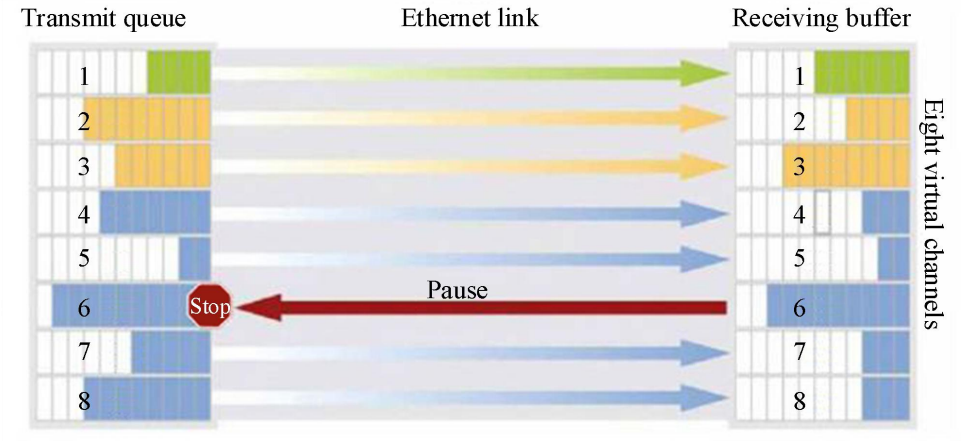


Figure 2-9 Priority-based Flow Control

2.12.2 Topology

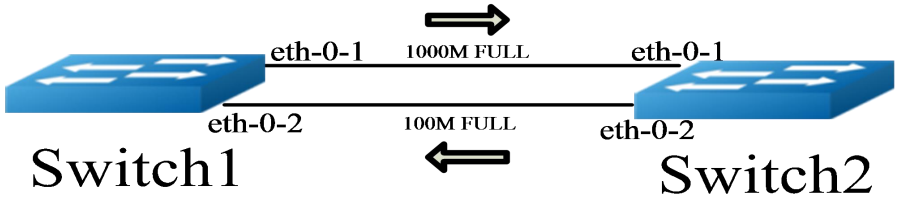


Figure 2-10 Priority-based Flow Control

2.12.3 Configure Enabling PFC Function

Switch1# configure terminal	Enter configuration mode
Switch1(config)# lldp enable	Globally enable lldp
Switch1(config)# interface eth-0-1	Enter interface mode
Switch1(config-if)#lldp enable	Enable 11dp under the interface
Switch1(config-if)# lldp tlv 8021-org-specific dcbx	Enable dcbx tlv under the interface
Switch1(config-if)# priority-flow-control mode on	Enable PFC on Port 1, without no need to negotiate with the opposite end
Switch1(config-if)# priority-flow-control enable priority 2 3 4	Configure enabling PFC at priority 2, 3, 4
Switch1(config)# interface eth-0-2	Enter interface mode
Switch1(config-if)#lldp enable	Enable 11dp under the interface
Switch1(config-if)# lldp tlv 8021-org-specific dcbx	Enable dcbx tlv under the interface
Switch1(config-if)# priority-flow-control mode auto	Enable PFC on Port 2, with the need to negotiate with the opposite end
Switch1(config-if)# priority-flow-control enable priority 2 3 4	Configure enabling PFC at priority 2, 3, 4
Switch1 (config-if)# exit	Go back to configuration mode

Switch2# configure terminal	Enter configuration mode
Switch2(config)# lldp enable	Globally enable lldp
Switch2(config)# interface eth-0-1	Enter interface mode

Switch2(config-if)#lldp enable	Enable 11dp under the interface
Switch2(config-if)# lldp tlv 8021-org-specific dcbx	Enable dcbx tlv under the interface
Switch2(config-if)# priority-flow-control mode on	Enable PFC on Port 1, without no need to negotiate with the opposite end
Switch2(config-if)# priority-flow-control enable priority 2 3 4	Configure enabling PFC at priority 2, 3, 4
Switch2(config)# interface eth-0-2	Enter interface mode
Switch2(config-if)#lldp enable	Enable 11dp under the interface
Switch2(config-if)# lldp tlv 8021-org-specific dcbx	Enable dcbx tlv under the interface
Switch2(config-if)# priority-flow-control mode auto	Enable PFC on Port 2, with the need to negotiate with the opposite end
Switch2(config-if)# priority-flow-control enable priority 2 3 4	Configure enabling PFC at priority 2, 3, 4
Switch2 (config-if)# exit	Go back to configuration mode

Flow control is valid on full-duplex links only

2.12.4 Configuration Validation

Switch2# show priority-flow-control

Port	PFC-enable		PFC-enable on priority		RxPause	TxPause
	admin	oper	admin	oper		
eth-0-1	on	on	234	234	0	0
eth-0-2	auto	off	234	off	0	0
eth-0-3	off	off	off	off	0	0
eth-0-4	off	off	off	off	0	0
eth-0-5	off	off	off	off	0	0
eth-0-6	off	off	off	off	0	0
eth-0-7	off	off	off	off	0	0
eth-0-10	off	off	off	off	0	0
eth-0-11	off	off	off	off	0	0
eth-0-12	off	off	off	off	0	0
eth-0-13	off	off	off	off	0	0
eth-0-14	off	off	off	off	0	0
eth-0-15	off	off	off	off	0	0
eth-0-16	off	off	off	off	0	0
eth-0-17	off	off	off	off	0	0
eth-0-18	off	off	off	off	0	0
eth-0-19	off	off	off	off	0	0
eth-0-20	off	off	off	off	0	0

2.13 Storm Control Configuration

2.13.1 Overview

Storm control refers to preventing flooding from consuming excessive switch resources by limiting maximum broadcast, maximum unknown multicast and maximum unicast flows received via designated interface, to ensure normal service operation.

Storm control can be realized as below:

- Level
- PPS

2.13.2 Terms

PPS: is short for packets per second.

2.13.3 Configure Storm Control by Means of Level

I. Layer-2-port-based configuration

Switch 1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# storm-control unicast level 0.1	Set unknown unicast message level to be controlled
Switch(config-if)# storm-control multicast level 1	Set multicast message level to be controlled
Switch(config-if)# storm-control broadcast level 10	Set broadcast message level to be controlled
Switch(config-if)# end	Exit to EXEC mode
Switch# show storm-control interface eth-0-1	Show storm control configuration details on the interface

II.Command validation

Switch# show storm-control interface eth-0-1

```
Port     ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 Level          0.10 Level          10.00 Level          1.00
```

2.13.4 Configure Storm Control by Means of PPS

I. Layer-2-port-based configuration

Switch 1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# storm-control unicast pps 1000	Set 1000 unknown unicast packets per second
Switch(config-if)# storm-control multicast pps 10000	Set 10000 multicast packets per second
Switch(config-if)# storm-control broadcast pps 100000	Set 100000 broadcast packets per second
Switch(config-if)# end	Exit to EXEC mode
Switch# show storm-control interface eth-0-1	Show storm control configuration details on the interface

II.Command validation

Switch# show storm-control interface eth-0-1

Port ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 PPS 1000 PPS 100000 PPS 10000

2.14 L2 Protocol Tunnel Configuration

2.14.1 Introduction

Customers enjoying connections via providers' network on various sites need to be able to run Layer 2 protocols normally. From this need providers' network is expected to transparently transmit STP/RSTP/MSTP packets, so that customers can overcome providers' network to construct their own STP trees and cut off redundant link.

If the Layer 2 protocol packet transparent transfer function is enabled, the switches on the edge of provider's network will encapsulate Layer 2 protocol packet with a new Layer 2 header and transmit to the provider's network. The encapsulated packet is transmitted as an ordinary packet in the provider's network. The newly-added Layer 2 header of the packet will be peeled off when the packet reaching the edge of the provider's network, and the Layer 2 protocol packet will be forwarded to user's switch for processing.

The Layer 2 protocol packet transparent transfer function can be utilized either separately or with QinQ feature.

2.14.2 Configure Layer 2 Protocol Messages Assigned for Transparent Transmission

I. Introduction

The assigned Layer 2 protocol messages include STP BPDU message, Slow proto message, 802.1X EAPOL message and CFM message.

Switch1 eth-0-1 and Switch2 eth-0-1 are configured as tunnel port in the example below. Switch1 eth-0-2 and Switch2 eth-0-2 are configured as uplink port. If the messages set forth above are received via Switch1 eth-0-1, the messages will come with a new Layer 2 header from the uplink port. In the new Layer 2 header: source MAC is tunnel dmac; source MAC is route-mac of the switch; VLAN id is corresponding to tunnel evc; VLAN priority is the configured Layer 2 protocol cos; Ethertype is OxFFEE. If the messages set forth above are received via Switch2 eth-0-2, the new Layer 2 header will be peeled off and the messages come from Switch2 eth-0-1.

II. Topology

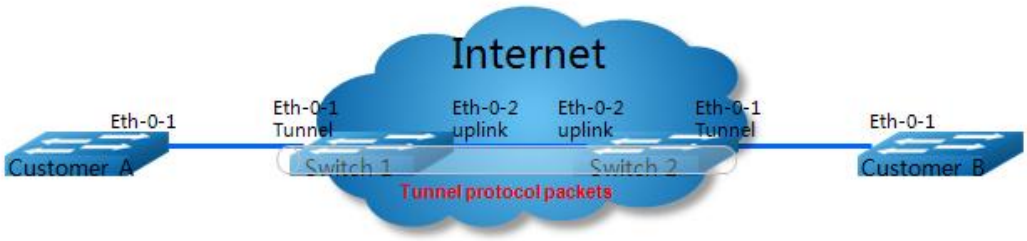


Figure 2-11 Topological Graph of L2 Protocol Tunnel

III. Configuration

Configure Switch 1 and Switch 2 with the commands listed in the table below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 2-5	Create vlan 2-5
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Configure the corresponding vlan id of evc_c1 as 2
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Configure the corresponding vlan id of evc_c2 as 3
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 4	Configure the corresponding vlan id of evc_c3 as 4

Switch(config)# ethernet evc evc_c4	Create EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 5	Configure the corresponding vlan id of evc_c3 as 5
Switch(config)# l2protocol enable	Globally enable Layer 2 protocol message transparent transmission
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	Globally configure tunnel dmac
Switch(config)# interface eth-0-1	Enter port mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport mode trunk	Configure the port as trunk
Switch(config-if)# switchport trunk allowed vlan add 2-5	Set the port to allow vlan 2-5
Switch(config-if)# spanning-tree port disable	Disable STP on the port
Switch(config-if)# l2protocol stp tunnel evc evc_c1	Configure tunneling stp bpdu to evc_c1
Switch(config-if)# l2protocol slow-proto tunnel evc evc_c2	Configure tunneling slow protocol to evc_c2
Switch(config-if)# l2protocol dot1x tunnel evc evc_c3	Configure tunneling dot1x eapol to evc_c3
Switch(config-if)# l2protocol cfm tunnel evc evc_c4	Configure tunneling cfm to evc_c4
Switch(config)# interface eth-0-2	Enter port mode
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# switchport mode trunk	Configure the port as trunk
Switch(config-if)# switchport trunk allowed vlan add 2-5	Set the port to allow vlan 2-5
Switch(config-if)# l2protocol uplink enable	Configure the port as uplink port of Layer 2 protocol message transparent transmission

IV. Configuration verification

Switch1# show l2protocol interface eth-0-1

```
Interface  PDU Address     MASK          Status     EVC
=========  ==============  ============  =========  ===============
```

```
eth-0-1   stp          FFFF.FFFF.FFFF  Tunnel   evc_c1
eth-0-1   slow-proto   FFFF.FFFF.FFFF  Tunnel   evc_c2
eth-0-1   dot1x        FFFF.FFFF.FFFF  Tunnel   evc_c3
eth-0-1   cfm          FFFF.FFFF.FFFF  Tunnel   evc_c4
```

Switch1# show l2protocol interface eth-0-2

```
Interface  PDU Address    MASK          Status   EVC
=========  =============  ============  =======  ===============
eth-0-2   stp          FFFF.FFFF.FFFF  Peer     N/A
eth-0-2   slow-proto   FFFF.FFFF.FFFF  Peer     N/A
eth-0-2   dot1x        FFFF.FFFF.FFFF  Peer     N/A
eth-0-2   cfm          FFFF.FFFF.FFFF  Peer     N/A
eth-0-2   N/A          N/A             Uplink   N/A
```

Switch1# show l2protocol tunnel-dmac

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

2.14.3 Configure Configurable Layer 2 Protocol Messages for Transparent Transmission

I. Introduction

Configurable Layer 2 protocol messages refer to messages with an address range of 0180.c200.0000 – 0x0180.c2ff.ffff.

Full mac address protocol messages refer to messages with an address range of 0000.0000.0000 – ffff.ffff.fff.

Switch1 eth-0-1 and Switch2 eth-0-1 are configured as tunnel port in the example below. Switch1 eth-0-2 and Switch2 eth-0-2 are configured as uplink port. If the protocol messages received via Switch 1 eth -0-1 comply with the configured mac address, the messages will come with a new Layer 2 header from the uplink port. In the new Layer 2 header: source MAC is tunnel dmac; source MAC is route-mac of the switch; VLAN id is corresponding to tunnel evc; VLAN priority is the configured Layer 2 protocol cos; Ethertype is OxFFEE. If messages with a new Layer 2 header are received via Switch2 eth-0-2, the new Layer 2 header will be peeled off and the messages come from Switch2 eth-0-1.

II. Topology

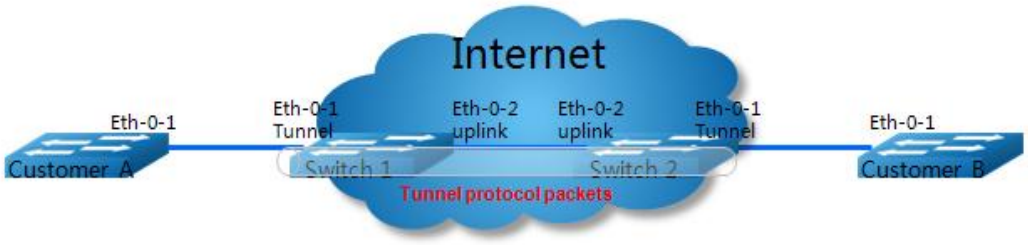


Figure 2-12 Topological Graph of L2 Protocol Tunnel

III. Configuration

Configure Switch 1 and Switch 2 with the commands listed in the table below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 2-4	Create vlan 2-4
Switch(config)# ethernet evc evc_c1	Create EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	Configure the corresponding vlan id of evc_c1 as 2
Switch(config)# ethernet evc evc_c2	Create EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	Configure the corresponding vlan id of evc_c2 as 3
Switch(config)# ethernet evc evc_c3	Create EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 4	Configure the corresponding vlan id of evc_c2 as 4
Switch(config)# l2protocol enable	Globally enable Layer 2 protocol message transparent transmission
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	Globally configure tunnel dmac
Switch1(config)# l2protocol mac 3 0180.C200.0008	Configure the mac address of Layer 2 protocol message 3 available for transparent transmission as 0180.C200.0008
Switch1(config)# l2protocol mac 4 0180.C200.0009	Configure the mac address of Layer 2 protocol message 4 available for transparent transmission as 0180.C200.0009
Switch1(config)# l2protocol full-mac 0100.0CCC.CCCC	Configure the full mac address available for transparent transmission as 0100.0CCC.CCCC
Switch(config)# interface eth-0-1	Enter port mode
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# switchport mode trunk	Configure the port as trunk
Switch(config-if)# switchport trunk allowed vlan add 2-4	Set the port to allow vlan 2-4
Switch(config-if)# spanning-tree port disable	Disable STP on the port

Switch(config-if)# l2protocol mac 3 tunnel evc evc_c1	Configure transparent transmission of Layer 2 protocol message 3 to evc_c1
Switch(config-if)# l2protocol mac 4 tunnel evc evc_c2	Configure transparent transmission of Layer 2 protocol message 4 to evc_c2
Switch(config-if)# l2protocol full-mac tunnel evc evc_c3	Configure transparent transmission of full mac address to evc_c3
Switch(config)# interface eth-0-2	Enter port mode
Switch(config-if)# no shutdown	Open the port
Switch(config-if)# switchport mode trunk	Configure the port as trunk
Switch(config-if)# switchport trunk allowed vlan add 2-4	Set the port to allow vlan 2-4
Switch(config-if)# l2protocol uplink enable	Configure the port as uplink port of Layer 2 protocol message transparent transmission

IV. Configuration validation

Switch1# show l2protocol interface eth-0-1

```
Interface  PDU Address     MASK           Status    EVC
=========  ==============  ==============  ========  ================
eth-0-1    0180.c200.0008  FFFF.FFFF.FFFF  Tunnel    evc_c1
eth-0-1    0180.c200.0009  FFFF.FFFF.FFFF  Tunnel    evc_c2
eth-0-1    0100.0ccc.cccc  FFFF.FFFF.FFFF  Tunnel    evc_c3
eth-0-1    stp             FFFF.FFFF.FFFF  Peer      N/A
eth-0-1    slow-proto      FFFF.FFFF.FFFF  Peer      N/A
eth-0-1    dot1x           FFFF.FFFF.FFFF  Peer      N/A
eth-0-1    cfm             FFFF.FFFF.FFFF  Peer      N/A
```

Switch1# show l2protocol interface eth-0-2

```
Interface  PDU Address     MASK           Status    EVC
=========  ==============  ==============  ========  ================
eth-0-2    0180.c200.0008  FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    0180.c200.0009  FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    0100.0ccc.cccc  FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    stp             FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    slow-proto      FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    dot1x           FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    cfm             FFFF.FFFF.FFFF  Peer      N/A
eth-0-2    N/A             N/A             Uplink    N/A
```

Switch1# show l2protocol tunnel-dmac

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

2.15 MSTP Configuration

2.15.1 Introduction

MST (Multiple Spanning Tree) is obtained by expanding RST (Rapid Spanning Tree) of IEEE802.1w. MST allows construction of multiple spanning trees via trunk link and association of VLANs with related spanning tree instances that are provided with a unique topological structure respectively. MST provides multiple data forwarding paths and load balancing, which enhances network fault tolerance. This is because the fault of one instance (forwarding path) will not impact other instances (forwarding path). One spanning tree instance can exist in the bridge assigned for consistent VLAN instances. Configuration of a set of bridges must be completed with the same MST configuration information so that these bridges belong to the same set of spanning tree instances, and interlinked bridges with the same MST configuration information constitute an MST Region.

MSTP trims the ring network into a loop-free tree network to avoid multiplication and endless loop of messages as in ring network, and also provides multiple redundant data forwarding paths to realize load balancing of VLAN data in the process of data forwarding. MSTP is compatible with STP and RSTP and can remedy the limitation of STP and of RSTP. It is capable of rapid convergence and making flows from different VLANs be distributed along their respective paths, so as to provide a better load sharing mechanism for redundant link.

2.15.2 Topology

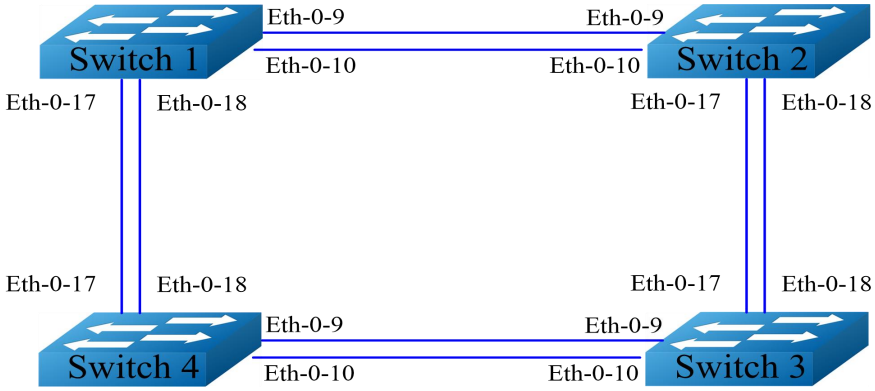


Figure 2-13 LACP Topology Example

2.15.3 Configuration

For purpose of the configuration example, it is assumed that you are running Layer 2 protocols. If you use non-Layer-2 protocol, you must set Layer 2 protocol by running switch port commands on each port.

Switch 1 – Switch 4

Switch# configure terminal	Enter configuration mode
Switch(config)# spanning-tree mode mstp	Configure STP mode

Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 10	Create VLAN10
Switch(config-vlan)# vlan 20	Create VLAN20
Switch(config-vlan)# exit	Exit VLAN mode
Switch(config)# spanning-tree mst configuration	Enter MSTP configuration mode
Switch(config-mst)# region RegionName	Configure MSTP region name
Switch(config-mst)# instance 1 vlan 10	Configure MSTP instance 1 to be associated with VLAN10
Switch(config-mst)# instance 2 vlan 20	Configure MSTP instance 2 to be associated with VLAN10
Switch(config-mst)# exit	Exit MSTP configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk
Switch(config-if)# switchport trunk allowed vlan all	Set the trunk to allow all VLANs
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-10	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk
Switch(config-if)# switchport trunk allowed vlan all	Set the trunk to allow all VLANs
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk mode
Switch(config-if)# switchport trunk allowed vlan all	Set the trunk to allow all VLANs
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-18	Enter interface mode
Switch(config-if)# switchport mode trunk	Set the interface as trunk mode

Switch(config-if)# switchport trunk allowed vlan all	Set the trunk to allow all VLANs
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# exit	Exit configuration mode

Switch 1

Switch# configure terminal	Enter configuration mode
Switch(config)# spanning-tree priority 0	Set STP priority as 0
Switch(config)# spanning-tree enable	Enable STP, which is disabled by default

Switch 2

Switch# configure terminal	Enter configuration mode
Switch(config)# spanning-tree instance 1 priority 0	Set STP instance 1 priority as 0
Switch(config)# spanning-tree enable	Enable STP, which is disabled by default

Switch 3

Switch# configure terminal	Enter configuration mode
Switch(config)# spanning-tree instance 2 priority 0	Set STP instance 2 priority as 0
Switch(config)# spanning-tree enable	Enable STP, which is disabled by default

Switch 4

Switch# configure terminal	Enter configuration mode
Switch(config)# spanning-tree enable	Enable STP, which is disabled by default

2.15.4 Command Validation

Step 1 Verify the status of MSTP interface of Switch 1.

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority      0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority      0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
            Aging Time  300 sec
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Designated     Forwarding     20000          128.9       P2p
eth-0-10     Designated     Forwarding     20000          128.10      P2p
eth-0-17     Designated     Forwarding     20000          128.17      P2p
eth-0-18     Designated     Forwarding     20000          128.18      P2p
##### MST1:  Vlans: 10
Root ID     Priority      1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     2225.fa28.c900
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Rootport       Forwarding     20000          128.9       P2p
eth-0-10     Alternate      Discarding     20000          128.10      P2p
eth-0-17     Designated     Forwarding     20000          128.17      P2p
eth-0-18     Designated     Forwarding     20000          128.18      P2p
##### MST2:  Vlans: 20
Root ID     Priority      2 (0x0002)
              Address     304c.275b.b200
Bridge ID   Priority    32770 (0x8002)
              Address     2225.fa28.c900
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Alternate      Discarding     20000          128.9       P2p
eth-0-10     Alternate      Discarding     20000          128.10      P2p
eth-0-17     Rootport       Forwarding     20000          128.17      P2p
eth-0-18     Alternate      Discarding     20000          128.18      P2p
```

Step 2 Verify the status of MSTP interface of Switch 2.

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority      0 (0x0000)
            Address     2225.fa28.c900
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
```

```
        Address    9c9a.7d91.9f00
        llo Time  2 sec  Max Age  20 sec Forward Delay 15 sec
        Aging Time  300 sec
Interface   Role        State         Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9     Rootport      Forwarding    20000        128.9      P2p
eth-0-10    Alternate     Discarding    20000        128.10     P2p
eth-0-17    Designated    Forwarding    20000        128.17     P2p
eth-0-18    Designated    Forwarding    20000        128.18     P2p
##### MST1:  Vlans: 10
Root ID     Priority      1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority      1 (0x0001)
            Address     9c9a.7d91.9f00
Interface   Role        State         Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9     Designated    Forwarding    20000        128.9      P2p
eth-0-10    Designated    Forwarding    20000        128.10     P2p
eth-0-17    Designated    Forwarding    20000        128.17     P2p
eth-0-18    Designated    Forwarding    20000        128.18     P2p
##### MST2:  Vlans: 20
Root ID     Priority      2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority    32770 (0x8002)
            Address     9c9a.7d91.9f00
Interface   Role        State         Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9     Designated    Forwarding    20000        128.9      P2p
eth-0-10    Designated    Forwarding    20000        128.10     P2p
eth-0-17    Rootport      Forwarding    20000        128.17     P2p
eth-0-18    Alternate     Discarding    20000        128.18     P2p
```

Step 3 Verify the status of MSTP interface of Switch 3.

Switch# show spanning-tree mst brief

```
##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority      0 (0x0000)
        Address     2225.fa28.c900
        Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
        Address     304c.275b.b200
        Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
        Aging Time  300 sec
Interface   Role        State         Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9     Rootport      Forwarding    20000        128.9      P2p
eth-0-10    Alternate     Discarding    20000        128.10     P2p
eth-0-17    Alternate     Discarding    20000        128.17     P2p
eth-0-18    Alternate     Discarding    20000        128.18     P2p
##### MST1:  Vlans: 10
Root ID     Priority      1 (0x0001)
        Address     9c9a.7d91.9f00
```

```
Bridge ID   Priority    32769 (0x8001)
          Address     304c.275b.b200
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Designated     Forwarding      20000         128.9        P2p
eth-0-10     Designated     Forwarding      20000         128.10       P2p
eth-0-17     Rootport       Forwarding      20000         128.17       P2p
eth-0-18     Alternate      Discarding      20000         128.18       P2p
##### MST2:  Vlans: 20
Root ID     Priority      2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority      2 (0x0002)
            Address     304c.275b.b200
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Designated     Forwarding      20000         128.9        P2p
eth-0-10     Designated     Forwarding      20000         128.10       P2p
eth-0-17     Designated     Forwarding      20000         128.17       P2p
eth-0-18     Designated     Forwarding      20000         128.18       P2p
```

Step 4 Verify the status of MSTP interface of Switch 4.

Switch# show spanning-tree mst brief

```
s##### MST0:  Vlans: 1
Multiple spanning tree protocol Enabled
Root ID     Priority      0 (0x0000)
            Address     2225.fa28.c900
          Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID   Priority    32768 (0x8000)
            Address     80a4.be55.6400
            Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
          Aging Time  300 sec
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Designated     Forwarding      20000         128.9        P2p
eth-0-10     Designated     Forwarding      20000         128.10       P2p
eth-0-17     Rootport       Forwarding      20000         128.17       P2p
eth-0-18     Alternate      Discarding      20000         128.18       P2p
##### MST1:  Vlans: 10
Root ID     Priority      1 (0x0001)
            Address     9c9a.7d91.9f00
Bridge ID   Priority    32769 (0x8001)
            Address     80a4.be55.6400
Interface    Role         State          Cost     Priority.Number    Type
--------------------------------------------------------------------------------
eth-0-9      Alternate      Discarding      20000         128.9        P2p
eth-0-10     Alternate      Discarding      20000         128.10       P2p
eth-0-17     Rootport       Forwarding      20000         128.17       P2p
eth-0-18     Alternate      Discarding      20000         128.18       P2p
##### MST2:  Vlans: 20
Root ID     Priority      2 (0x0002)
            Address     304c.275b.b200
Bridge ID   Priority    32770 (0x8002)
```

```
                Address    80a4.be55.6400
Interface   Role        State          Cost     Priority.Number     Type
--------------------------------------------------------------------------------
eth-0-9     Rootport    Forwarding     20000        128.9           P2p
eth-0-10    Alternate   Discarding     20000        128.10          P2p
eth-0-17    Designated  Forwarding     20000        128.17          P2p
eth-0-18    Designated  Forwarding     20000        128.18          P2p
```

2.16 MLAG Configuration

2.16.1 Introduction

In a high reliability data center topology, it is typical to connect TOR switch with server via two aggregate switches to provide redundancy protection. In such topological structure, spanning tree protocols aggregate half interfaces of switches via block to prevent network loops, at the cost of bandwidth reduction by 50%.

This problem can be solved by deploying MLAG. Connect the two aggregate switches via an MLAG link to make them as one device logically. The ports of the two devices form aggregation ports together, so that all ports can participate in data flow forwarding together.

MLAG has the following benefits:

- Providing higher bandwidth at the time of network traffic increase;
- Making full use of network bandwidth by reducing the ports blocked by STP;
- Connecting other switches or servers via static LAG or LACP, without the aid of other protocols;
- Supporting loop prevention via spanning tree protocol

2.16.2 Topology

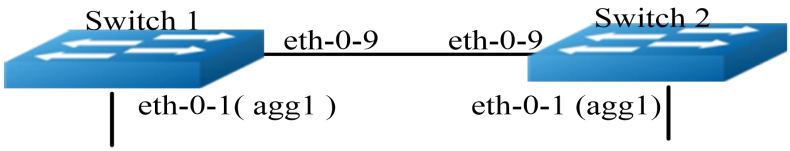


Figure 2-14 MLAG Configuration Topology

2.16.3 Configuration

Configure Switch1

Switch1 (config)# vlan database	Enter vlan mode
Switch1 (config-vlan)# vlan 10,4094	Create vlan10 and vlan4094

Switch1(config-vlan)# exit	Exit vlan mode and go back to global configuration mode
Switch1(config)# interface eth-0-1	Enter interface configuration mode
Switch1(config-if)# static-channel-group 1	Add the interface into static group agg1
Switch1(config-if)# no shutdown	Configure interface up
Switch1(config-if)# exit	Exit interface configuration mode and go back to global configuration mode
Switch1(config)# interface eth-0-9	Enter interface configuration mode
Switch1(config-if)# switchport mode trunk	Configure the interface as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Allow all vlans at this trunk
Switch1(config-if)# spanning-tree port disable	Disable spanning tree protocol on the port
Switch1(config-if)# no shutdown	Configure interface up
Switch1(config-if)# exit	Exit interface configuration mode and go back to global configuration mode
Switch1 (config)# interface agg1	Enter agg1 interface mode
Switch1(config-if)# switchport mode trunk	Configure as trunk port
Switch1(config-if)# switchport trunk allowed vlan add 10	Allow vlan10 on this interface
Switch1(config-if)# mlag 1	Associate this interface with mlag1
Switch1(config-if)# exit	Exit interface configuration mode and go back to global configuration mode
Switch1 (config)# interface vlan4094	Create Layer 3 interface vlan 4094
Switch1(config-if)# ip address 12.1.1.1/24	Configure IP address as 12.1.1.1/24
Switch1(config-if)# exit	Exit interface configuration mode and go back to global configuration mode
Switch1 (config)# mlag configuration	Enter mlag configuration mode
Switch1 (config-mlag)# peer-link eth-0-9	Configure peer link
Switch1 (config-mlag)# peer-address 12.1.1.2	Configure peer neighbor address
Switch1 (config-mlag)# exit	Exit mlag mode and go back to global configuration mode

Configure Switch2

Switch2 (config)# vlan database	Enter vlan mode
Switch2 (config-vlan)# vlan 10,4094	Create vlan10 and vlan4094
Switch2(config-vlan)# exit	Go back to global configuration mode
Switch2(config)# interface eth-0-1	Enter interface mode
Switch2(config-if)# static-channel-group 1	Add the interface intto static agg1
Switch2(config-if)# no shutdown	Enable interface up
Switch2(config-if)# exit	Go back to global configuration mode
Switch2(config)# interface eth-0-9	Enter interface mode
Switch2(config-if)# switchport mode trunk	Set the interface as trunk
Switch2(config-if)# switchport trunk allowed vlan all	Allow all vlans on this trunk port
Switch2(config-if)# spanning-tree port disable	Disable spanning tree protocol on this port
Switch2(config-if)# no shutdown	Enable interface up
Switch2(config-if)# exit	Go back to global configuration mode
Switch2 (config)# interface agg1	Enter agg interface mode
Switch2(config-if)# switchport mode trunk	Configure the interface as trunk
Switch2(config-if)# switchport trunk allowed vlan add 10	Allow vlan10 on this interface
Switch2(config-if)# mlag 1	Bind this interface with mlag1
Switch2(config-if)# exit	Go back to global configuration mode
Switch2 (config)# interface vlan4094	Create interface vlan4094
Switch2(config-if)# ip address 12.1.1.2/24	Configure IP address 12.1.1.2/24
Switch2(config-if)# exit	Go back to global configuration mode
Switch2 (config)# mlag configuration	Enter mlag configuration mode
Switch2 (config-mlag)# peer-link eth-0-9	Configure peer link
Switch2 (config-mlag)# peer-address 12.1.1.1	Configure peer neighbor address
Switch2 (config-mlag)# end	Go back to privilege mode

2.16.4 Command Validation

Validate switch1

```
Switch1# show mlag
MLAG configuration:
-----------------
role              : Master
local_sysid   : ea90.aecc.cc00
mlag_sysid  : ea90.aecc.cc00
peer-link      : eth-0-9
peer conf      : Yes
Switch1# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
Switch1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:13:07
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 19 messages,Sent 23 messages
Open        : received 1, sent 2
KAlive      : received 15, sent 16
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 0
Conf        : received 1, sent 1
STP Total: received 2, sent 4
 Global    : received 2, sent 3
 Packet     : received 0, sent 0
 Instance  : received 0, sent 0
 State       : received 0, sent 1
Connections established 1; dropped 0
Local host   : 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 46157
remote_sysid: baa7.8606.8b00
Switch1# show mac address-table
         Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
Validate switch2
Switch2# show mlag
MLAG configuration:
-----------------
role        : Slave
local_sysid : baa7.8606.8b00
mlag_sysid  : ea90.aecc.cc00
peer-link   : eth-0-9
peer conf   : Yes
Switch2# show mlag interface
mlagid  local-if  local-state    remote-state
1       agg1      up             up
Switch2# show mlag peer
MLAG neighbor is 12.1.1.1, MLAG version 1
MLAG state = Established, up for 12:14:29 AM
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 23 messages,Sent 21 messages
```

```
Open       : received 1, sent 1
KAlive     : received 17, sent 17
Fdb sync   : received 0, sent 0
Failover   : received 0, sent 0
Conf       : received 1, sent 1
STP Total: received 4, sent 2
 Global    : received 3, sent 2
 Packet    : received 0, sent 0
 Instance : received 0, sent 0
 State     : received 1, sent 0
Connections established 1; dropped 0
Local host: 12.1.1.2, Local port: 46157
Foreign host: 12.1.1.1, Foreign port: 61000
remote_sysid: ea90.aecc.cc00
Switch2# show mac address-table
        Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

3 Device Management Configuration Guide

3.1 STM Configuration

3.1.1 Introduction

STM supports optimization of specific features by configuring system resources of switches. You can choose a configuration file to maximize the system functions, for instance, using a default configuration file to balance resources or using a VLAN configuration file to obtain maximum MAC entries. To make the most of TCAM resources in different situations, STM provides different system optimization functions. The current version supports the following STM templates:

- Layer3: routing template, supporting maximum number of routings and usually applied in the router or aggregation layer of the network center.
- Layer2: VLAN template, supporting maximum number of unicast MAC addresses. It is usually selected as a Layer2 switch.
- Default: default template, providing balancing of all features.
- Ipv6: ipv6 template, supporting ipv6 protocols and dual-stack usage of v4 and v6. It usually applies to ipv6 network.

If you has configured (or are using) an STM mode that doesn't exist in the next image to be enabled, default hard-coded configuration will be applied when the image is enabled, and the configuration might be different from the normal default mode.

3.1.2 Configuration

Select correct STM profiles by referring to the configuration guide:

- Switch rebooting is required after configuration changing.
- STM layer2 template is applied for layer2 switches on the occasion of no routing.
- It doesn't need to switch to layer3 template if the routing function is not enabled on the switch.

Switch# configure terminal	Enter configuration mode

Switch(config)# stm prefer layer3	Set STM profile as layer3
Switch(config)# end	Exit configuration mode
Switch# reload	Reboot

3.1.3 Command Validation

The example below shows the output results for the usage of routing template:

Switch# show stm prefer

```
Current profile is :default
  number of vlan instance                        : 1/4094
  number of unicast & multicast mac address   : 0/65536
  number of backhole mac address                 : 0/128
  number of max applied vlan mapping          : 0/1024
  number of mac based vlan class                 : 0/512
  number of ipv4 based vlan class                : 0/512
  number of dot1x mac based                      : 0/2048
  number of unicast ipv4 host routes             : 0/4096
  number of unicast ipv4 indirect routes         : 0/8192
  number of unicast ipv4 ecmp groups          : 0/256
  number of unicast ipv4 policy based routes : 0/16
  number of unicast ip tunnel peers              : 0/8
  number of multicast ipv4 routes                : 0/1023
  number of multicast ipv4 routes membe      : 0/1024
  number of ipv4 source guard entries            : 0/1024
  number of ipv4 acl/qos flow entries            : 0/511
  number of link aggregation (static & lacp)   : 0/55
The profile stored for use after the next reload is the layer3 profile.
  number of vlan instance                    : 1/4094
  number of unicast & multicast mac address : 0/32768
  number of backhole mac address             : 0/128
  number of max applied vlan mapping         : 0/1024
  number of mac based vlan class             : 0/512
  number of ipv4 based vlan class            : 0/1024
  number of dot1x mac based                  : 0/512
  number of unicast ipv4 host routes         : 0/20480
  number of unicast ipv4 indirect routes     : 0/8192
  number of unicast ipv4 ecmp groups         : 0/256
  number of unicast ipv4 policy based routes : 0/64
  number of unicast ip tunnel peers          : 0/8
  number of multicast ipv4 routes            : 0/1024
  number of multicast ipv4 routes member     : 0/1024
  number of ipv4 source guard entries        : 0/512
  number of ipv4 acl/qos flow entries        : 0/1536
  number of link aggregation (static & lacp)   : 0/55
  number of ipfix cache                      : 0/16384
```

3.2 System Log Configuration

3.2.1 Introduction

System messages can be stored in a log file or sent to other server devices. System message management module has the following functions:

- Recording log information to facilitate monitoring and troubleshooting
- Selecting the type of log information to be recorded
- Selecting log destination

By default, switches will record important system information in the internal buffer and send it to the system console. Users can specify the message level to be saved. Information will be attached with occurrence time to improve just-in-time debugging and manageability.

You can fetch system messages via CLI (Command Line Interface) of switches or by saving it to a log server. The log buffer of switches can store 1000 messages to the most. Users can conduct real time system log monitoring by logging in via Telnet or console port and turning on the terminal monitoring.

3.2.2 Terms

Logging: Current log configuration

Show: Show log configuration details

Levels: Security level information

Enable: Enable saving log to local file

Disable: Disable saving log to local file

Table 3-1 System Message Type

Name	Definition
kern	Kernel message
User	Random user level message
Mail	Mail system
daemon	System process
Auth	Security/authentication message
syslog	Generate internal system messages via syslogd
lpr	Lineprinter subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock process
authpriv	Private security/authentication message

Name	Definition
ftp	FTP process

Table 3-2 Definition of Security Level

Severity level	Definition
emergency	System is out of operation
alert	Must take actions immediately
critical	Critical event
error	Error event
warning	Warning event
notice	Normal but an important event
information	Information
debug	Debug

3.2.3 Configure Log Server

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# logging server enable	Enable LOG Server
Switch(config)# logging server address 1.1.1.1	Specify LOG Server Ipv4 address
Switch(config)# logging server address 2001:1000::2	Specify LOG Server Ipv6 address
Switch(config)# logging server severity debug	Set log record level
Switch(config)# logging server facility mail	Set log messages

II. Command validation

Switch# show logging

Current logging configuration:

==========

logging buffer 500
logging timestamp bsd
logging file enable
logging level file warning

logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging server address 2001:1000::2
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable

3.2.4 Set Log Buffer Size

By default, 500 latest log messages are saved in log buffer. Users can change the range between 10 to 1000 via running command.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# logging buffer 700	Set log buffer size as 700

II. Command validation

Switch# show logging

Current logging configuration:
==========

logging buffer 700
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable

You can check log configuration via command "show". For configuring syslog server, be sure to connect correctly, which can be guaranteed via mutual ping command between two computers. Users also need to configure syslog software on the log server to receive logs.

3.3 Mirror Configuration

3.3.1 Introduction

Users can make a copy of messages receiving or sending via a certain port or VLAN, send it out from another port of the device, and link the port to a tester or other message collection gathering equipment, to attain the goal of capturing and analyzing original messages.

Only messages received and sent via a designated port or designated VLAN can be mirrored, and such port or VLAN is called mirror source. The mirror function is for monitoring mirror sources rather than traffic sources. For example, in the case of mirroring incoming traffic to a VLAN, the messages forwarded from other VLANs to this VLAN will not be copied, while the traffic received via this VLAN to be forwarded to other VLANs will be copied.

The mirror function will not affect the initial network traffic of the source port or source VLAN of switches; the messages sent or received via the source port can be copied, and the copy of traffic will be sent to a designated destination port.

3.3.2 Terms

The concepts and terms related to mirror configuration are described below:

Mirror Session

Mirror session refers to a collection of a set of mirror sources and one mirror destination, where the mirror source can include any number of ports or VLANs, and layer2 or layer3 physical interface can be taken as mirror destination.

The system supports three mirror sessions to the most.

The mirror function should not interfere regular services.

In a mirror session, if the total flow of the mirror source is beyond the forwarding capacity of the mirror destination port (for example, using a destination port with a maximum rate of 10Mbps to monitor 100Mbps traffic), packet dropout will occur.

A mirror session that can work normally requires a mirror destination port and at least one mirror source.

Traffic Class

Mirror session relates to three traffic classes:

Mirror in the receiving direction (RX): Mirror of a port or VLAN in the receiving direction is to copy the traffic received via the port or VLAN fully and faithfully as far as possible before any modification and processing by the system in principle. The mirror source port has a limitation: messages with CRC error cannot be mirrored. The mirror source VLAN has a limitation: BPDU, LACPDU, BMGPDU messages, messages failed in IP-MAC binding check, and messages with CRC error cannot be mirrored. Message modification or discarding by any other functions of QOS including DSCP modification, VLAN translation, VLAN classification, ACL, VLAN's ingress filter, MAC filter, STP, VLAN tag control, port security, and unknown routing packets should not affect the mirror function in the receiving direction. The copy generated to the destination port must be identical with the messages received via the mirror source.

Mirror in the transmitting direction (TX): Mirror of a port or VLAN in the transmitting direction is to copy the traffic transmitted via the port or VLAN faithfully as far as possible in principle. The messages discarded before being transmitted from the port or VLAN will not be mirrored. Taking VLAN as mirror source has a limitation: the messages from CPU cannot be mirrored.

Both-way mirror (BOTH): In a mirror session, users can monitor the message flow of the same mirror source in both receiving and transmitting directions.

Mirror Source

Source port (also called monitored port) refers to a layer2 or layer3 port to be monitored or analyzed. Source VLAN (also called monitored VLAN) refers to a VLAN to be monitored or analyzed. In a mirror session, users can monitor the traffic of one or more mirror sources in the receiving direction (RX), transmitting direction (TX) or both way. The system supports mirror source ports of any number (equal to the maximum of available ports of the system) and mirror source VLANs of any number (equal to the maximum of available VLAN of the system).

Source port has the following features:

- Any type of port can be taken as source port (such as Ethernet port)
- Can be monitored in one mirror session only
- Cannot be taken as the destination port of any mirror session

The monitoring direction of every mirror source port or mirror source VLAN can be configured (incoming, outgoing or both-way). For a port aggregation group, the monitoring direction will apply to all physical ports in the group.

Mirror source ports can be in the same or different VLANs.

A VLAN port must be created to configure mirror source VLAN.

Any member port of an aggregation group cannot be individually configured as mirror source.

Destination Port

Each mirror session requires one destination port (also called monitoring port) to receive the mirrored messages.

Destination port has the following features:

- Destination port and mirror source must be on the same device.
- Any physical port can be taken as destination port.
- Any member port of an aggregation group cannot be configured as mirror destination port.
- Can be taken as destination port in one mirror session only.
- Cannot be configured as mirror source port of any mirror session.
- Destination port will not transmit any flow outside the mirror function.
- During the running of mirror session, STP cannot be applied to the destination port.
- The configurations related other system functions of destination port will retain out of service, until it stops acting as destination port of a mirror session.
- Mirror destination port will not learn MAC.

- The real-time rate/duplex status may be inconsistent with the displayed value.

3.3.3 Configuration

Mirror configuration is as below

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 10	Create VLAN
Switch(config-vlan)# exit	Exit VLAN configuration mode
Switch(config)# interface vlan10	Create VLAN interface
Switch(config-if)# exit	Exit VLAN interface configuration mode
Switch(config)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# monitor session 1 destination interface eth-0-2	Assign destination interface of a mirror session
Switch(config)# monitor session 1 source interface eth-0-1both	Specify mirror session, source interface and monitoring direction
Switch(config)# monitor session 1 source vlan 10 rx	Specify mirror session and source VLAN
Switch(config)# end	Exit global configuration mode
Switch# show monitor session 1	Show configuration

3.3.4 Command Validation

For purpose of this example, session 1 is created to monitor the traffic of the source port and source VLAN.

You can view the configuration with command "show session"

Switch # show monitor session 1

```
Session  1
---------
Status              : Valid
Type                : Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
```

```
Source VLANs    :
  Receive Only    : 10
  Transmit Only   :
  Both            :
Destination Port  : eth-0-2
```

3.4 Configuration of Mirror with Multiple Destination Ports

3.4.1 Introduction

Users can make a copy of messages receiving or transmitting via a certain port and transmit it from several other ports of the device, and link the ports to a tester or other message collection gathering equipment to attain the goal of capturing and analyzing original messages.

Only messages received and transmitted via the designated port can be mirrored, and such port is called mirror source. The mirror function is for monitoring mirror sources rather than traffic sources.

The mirror function will not affect the initial network traffic of source port of switches; the messages transmitted or received via the source port can be copied, and the copy of traffic will be transmitted to the designated destination port.

3.4.2 Configure

Mirror configuration is as below

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-3	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# monitor session 1 destination group 1	Create destination interface group of mirror session
Switch(config-monitor-d-group)# member eth-0-2	Add interface eth-0-2 into the

	destination port group
Switch(config-monitor-d-group)# member eth-0-3	Add interface eth-0-3 into the destination port group
Switch(config)# monitor session 1 source interface eth-0-1	Specify mirror session, source interface and monitoring direction
Switch(config)# end	Exit global configuration mode
Switch# show monitor session 1	Show configuration

3.4.3 Command Validation

For purpose of this example, session 1 is created to monitor the traffic of the source port.

You can view the configuration with the show session command

Switch # show monitor session 1

```
Session   1
---------
Status              :  Valid
Type                :  Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2 eth-0-3
```

3.5 Remote Mirror Configuration

3.5.1 Configure Remote Mirror

I. Introduction

Remote mirror function supports mirroring with source port (or source VLAN) and destination port on different devices to realize remote monitoring in a network across a set of devices.

II. Terms

The concepts and terms related to remote mirror configuration are described below:

Remote Mirror Session

Refers to a collection of a set of mirror sources and one remote mirror destination, where the remote mirror destination consists of one outbound physical interface and one VLAN.

The concepts of source port and VLAN in the case of remote mirror session are same with local mirror.

Remote mirror destination has the following features:

- A combination of a designated port and a VLAN
- Remote VLAN ranges from 2 to 4094. If no VLAN is created in the system, users cannot take the VLAN as remote mirror VLAN.
- The outbound port should be an ordinary physical port that needs to be configured by users to ensure the ability of transmitting mirror messages, and should not be interfered by flows of other functions.
- Messages from the mirror source will be tagged with the designated remote VLAN ID and transmitted from the designated outbound interface to a remote device.
- It is suggested to use layer2 interface as the remote mirror destination port. Additionally, users must add the port into the designated remote VLAN to transmit messages successfully.

III. Topology

As shown in Figure 3-1, the mirror source port is on Switch A, and the mirrored messages are encapsulated in a designated VLAN and transmitted to the remote device Switch B in various mirror sessions.

Same with a local session, a port or VLAN can be taken as the mirror source of a remote mirror session.

For remote mirror session, the destination port must be a physical port, and a VLAN must be assigned for encapsulating mirror messages.

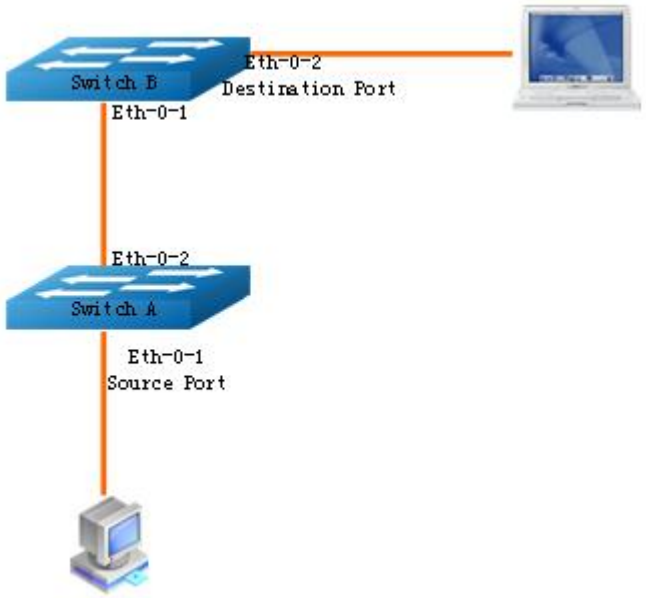


Figure 3-1 Remote Mirror

Configuration

The configuration of remote mirror on Switch A is as below:

SwitchA# configure terminal	Enter global configuration mode
SwitchA(config)# vlan database	Enter VLAN configuration mode
SwitchA(config-vlan)# vlan 10	Create VLAN 10
SwitchA(config-vlan)# vlan 15	Create VLAN 15
SwitchA(config-vlan)# exit	Exit VLAN configuration mode
SwitchA(config-if)# exit	Exit interface configuration mode
SwitchA(config)# interface eth-0-2	Enter interface configuration mode
SwitchA(config-if)# no shutdown	Interface up
SwitchA(config-if)# switchport mode trunk	Set port mode as trunk
SwitchA(config-if)# switchport trunk allowed vlan add 15	Add eth-0-2 into vlan 15
SwitchA(config-if)# exit	Exit interface configuration mode
SwitchA(config)# interface eth-0-1	Enter interface configuration mode
SwitchA(config-if)# switchport mode access	Set port mode as access
SwitchA(config-if)# switchport access vlan 10	Add eth-0-1 into vlan 10
SwitchA(config)# monitor session 1 destination	Specify mirror session, remote

remote vlan 15 interface eth-0-2	destination vlan and outbound port
SwitchA(config)# monitor session 1 source interface eth-0-1 both	Specify mirror session and source port (mirror port)
SwitchA(config)# end	Exit EXEC mode
SwitchA# show monitor session 1	Show configuration

Switch B Configuration

1. Run the command of “monitor session ID source vlan” to obtain a copy of tagged remote mirror messages.

SwitchB# configure terminal	Enter global configuration mode
SwitchB(config)# vlan database	Enter VLAN configuration mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-vlan)# exit	Exit VLAN configuration mode
SwitchB(config)# interface vlan15	Enter vlan configuration mode
SwitchB(config-if)# exit	Exit vlan configuration mode
SwitchB(config)# interface eth-0-2	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up
SwitchB(config-if)# switchport mode access	Set port mode as access
SwitchB(config-if)# switchport access vlan 15	Add eth-0-2 intto vlan 15
SwitchB(config)# interface eth-0-1	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up
SwitchB(config-if)# switchport mode trunk	Set port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 intto vlan 15
SwitchB(config-if)# exit	Exit interface configuration mode
SwitchB(config)# monitor session 1 destination interface eth-0-2	Specify mirror session and destination address
SwitchB(config)# monitor session 1 source vlan 15 rx	Specify mirror session and source VLAN
SwitchB(config)# end	Exit EXEC mode
SwitchB# show monitor session 1	Show configuration

2. Capture messages via access port (Switch B doesn't need configuration of any mirror session)

SwitchB# configure terminal	Enter global configuration mode
SwitchB(config)# no spanning-tree enable	Disable stp
SwitchB(config)# vlan database	Enter VLAN configuration mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-vlan)# exit	Exit VLAN configuration mode
SwitchB(config)# interface eth-0-2	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up
SwitchB(config-if)# switchport mode access	Set port mode as access
SwitchB(config-if)# switchport access vlan 15	Add eth-0-2 intto vlan 15
SwitchB(config)# interface eth-0-1	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up
SwitchB(config-if)# switchport mode trunk	Set port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 intto vlan 15
SwitchB(config-if)# exit	Exit interface configuration mode

3. Capture destination messages via trunk port (Switch B doesn't need configuration of any mirror session)

SwitchB# configure terminal	Enter global configuration mode
SwitchB(config)# no spanning-tree enable	Disable stp
SwitchB(config)# vlan database	Enter VLAN configuration mode
SwitchB(config-vlan)# vlan 15	Create VLAN 15
SwitchB(config-vlan)# exit	Exit VLAN configuration mode
SwitchB(config)# interface eth-0-2	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up
SwitchB(config-if)# switchport mode trunk	Set port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-2 into vlan 15
SwitchB(config)# interface eth-0-1	Enter interface configuration mode
SwitchB(config-if)# no shutdown	Interface up

SwitchB(config-if)# switchport mode trunk	Set port mode as trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	Add eth-0-1 into vlan 15
SwitchB(config-if)# exit	Exit interface configuration mode

Methods 2 and 3 will cause the system to learn mirror message MAC, which might lead to exhaustion of FDB table resources.

IV. Command validation

For purpose of this example, session 1 is created to monitor the traffic of the source port and source VLAN.

You can view the configuration with the show session command.

SwitchA# show monitor session 1

```
Session  1
---------
Status              : Valid
Type                :  Remote Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2
Destination remote VLAN : 15
SwitchB# show monitor session 1
Session  1
---------
Status              : Valid
Type                :  Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              :
Source VLANs        :
  Receive Only      : 15
  Transmit Only     :
  Both              :
Destination Port    : eth-0-2
```

3.5.2 Configure Mac Escape Remote Mirror

I. Introduction

MAC escape is a remote mirror subfunction that will affect the results of remote mirror only. An MAC escape entry consists of one MAC address and one MAC mask. Once an MAC escape entry is established, the entries matching MAC-DA messages will not be mirrored to the remote destination VLAN. Users can utilize MAC escape entries to prevent protocol messages from being mirrored to the remote.

Two MAC escape entries at most can be configured globally.

II. Configuration

SwitchA# configure terminal	Enter global configuration mode
SwitchA(config)# monitor mac escape 00cc.12A9.33D8 ffff.ffff.ffff	Establish mac escape entry
SwitchA(config)# monitor mac escape 00cc.159E.24F0 ffff.ffff.ffff	Establish another mac escape entry
SwitchA(config)# end	Exit global configuration mode
SwitchA# show monitor mac escape	Show mac escape configuration

III. Command validation

Mac escape entries have been established in this example.

You can view the configuration with the show command

SwitchA# show monitor mac escape

```
------------------------------------------------------------
        monitor rspan mac escape database
------------------------------------------------------------
count   : 2
------------------------------------------------------------
 Mac     : 00:cc:12:a9:33:d8
 Mask    : ff:ff:ff:ff:ff:ff
 Mac     : 00:cc:15:9e:24:f0
 Mask    : ff:ff:ff:ff:ff:ff
```

3.5.3 Configure ERSPAN Remote Mirror

I. Introduction

In some occasions of data processing, it is needed to transmit the data received and transmitted via some ports of switches via layer3 network to a remote analyzer for analyzing. ERSPAN allows transmitting data that is added with GRE header via GRE channel to an analyzer, and data transmission will not be affected during the monitoring process. If a large amount of data is transmitted, ERSPAN can distribute message load to several destination analyzing devices by settings for purpose of load reduction, as shown in Figure 5-3.

II. Topology

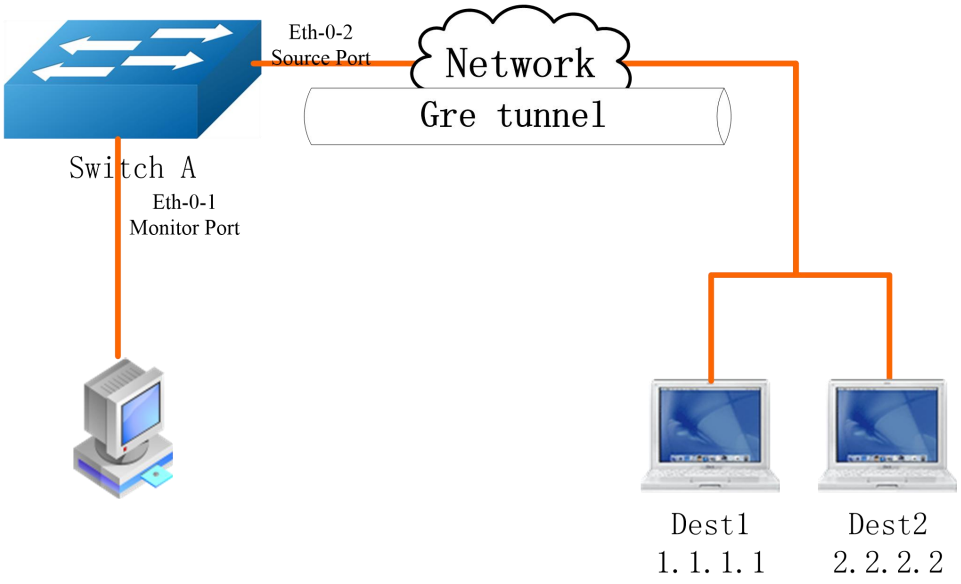


Figure 3-2 Erspan

III. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-2	Enter interface configuration mode
Switch(config-if)# no switchport	Set port mode as trunk
Switch(config-if)# ip address 10.10.10.1/24	Configure interface IP address
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface tunnel1	Create tunnel1 and enter its configuration mode
Switch(config-if)# tunnel source eth-0-2	Assign tunnel source port
Switch(config-if)# tunnel multi-destination 1.1.1.1	Specify tunnel destination IP address 1
Switch(config-if)# tunnel multi-destination 2.2.2.2	Specify tunnel destination IP address 2
Switch(config-if)# tunnel gre key 3333	Set gre key

Switch(config-if)# tunnel extend-header (dst-lod-balance|)	Set extend header
Switch(config-if)# tunnel mode (multi-dst-gre|gre)	Set tunnel mode
Switch(config-if)# exit	Exit tunnel1 configuration mode
Switch(config)# arp 10.10.10.2 0000.0000.0001	Arp information setting
Switch(config)# arp 11.11.11.2 0000.0000.0002	Arp information setting
Switch(config)# ip route 1.1.1.0/24 10.10.10.2	Routing information setting
Switch(config)# ip route 2.2.2.0/24 10.10.10.2	Routing information setting
Switch(config)# monitor session 1 destination interface tunnel1	Assign the destination interface of a mirror session
Switch(config)# monitor session 1 source interface eth-0-1both	Assign the source interface of a mirror session
Switch(config)# end	Exit global configuration mode
Switch# show monitor session 1	Show configuration of session 1
Switch#show running-config interface tunnel 1	Show tunnel configuration details

IV. Command validation

```
SwitchA# show monitor mac escape
Session   1
----------
Status              : Valid
Type                : Local Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : tunnel1
SwitchA# show running-config interface tunnel 1
Building configuration...
!
interface tunnel1
 tunnel source eth-0-2
 tunnel multi-destination 1.1.1.1
 tunnel multi-destination 2.2.2.2
 tunnel gre key 3333
 tunnel multi-dst-gre extend-header
 tunnel mode multi-dst-gre
!
```

3.6 Destination Port Configuration of CPU Mirror

3.6.1 Introduction

Users can make a copy of messages receiving or sending via a certain port or VLAN and transmit it out from another port of the device, and link the port to a tester or other message collection gathering equipment to attain the goal of capturing and analyzing original messages. If the port is unable to link to a tester or other message gathering equipment or the equipment resources are short, the copied messages need to be transmitted to the CPU and saved for rapid analysis by users or programmers. Making a copy of messages and transmitting it to the CPU is an approach coping with hardware resource shortage. The rate of transmitting mirrored messages up to the CPU is the system default limit rate or can be specified by users.

3.6.2 Configuration

1. Configure the cpu as the mirror destination port, eth-0-1 as the mirror source, and the direction as both-way; configure the size of memory storage of mirror cpu as 100 packets; configure the limit rate of mirror cpu as 128pps.

Switch# configure terminal	Enter configuration mode
Switch(config)# monitor session 1 destination cpu	Configure cpu as the mirror destination port of session 1
Switch(config)# monitor session 1 source interface eth-0-1both	Configure eth-0-1 as the mirror source of session 1 and the direction as both-way (also both-way by default)
Switch(config)# monitor cpu set packet buffer 100	Configure the size of memory storage of mirror cpu as 100 packets, and the maximum as 100 packets
Switch Switch(config)# cpu-traffic-limit reason mirror-to-cpu rate 128	Configure the mirror-cpu packet rate as 128pps
Switch# exit	Exit global configuration mode

2. Configure the capture strategy of the mirror cpu as drop with replace as the default value.

Switch(config)# monitor cpu capture strategy drop	Configure the capture strategy of mirror cpu as drop. (Namely, new packets will be dropped if the memory space is filled.)
Switch(config)# monitor cpu capture strategy replace	Configure the capture strategy of mirror cpu as replace. (Namely, new packets will replace legacy packets if the memory space is filled.)

3.6.3 Command Validation

1. Session 1 has been created in the example for monitoring the traffic of the source port eth-0-1, and the mirror to cpu messages can be viewed by running the show command. The configuration can be viewed by running the show command:

```
Switch# show monitor session 1
DUT1# show monitor session 1
Session   1
---------
Status              : Valid
Type                : Cpu Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : eth-0-1
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : cpu
```

2. View packets stored in the memory after mirror-to-cpu transmission of messages

```
DUT1# show monitor cpu packet all
-----------------show all mirror to cpu packet info-----------------
packet: 1
Source port: eth-0-1
MACDA:264e.ad52.d800, MACSA:0000.0000.1111
vlan tag:100
IPv4 Packet, IP Protocol is 0
IPDA:3.3.3.3, IPSA: 10.0.0.2
Data length: 47
Data:
 264e ad52 d800 0000 0000 1111 8100 0064
 0800 4500 001d 0001 0000 4000 6ad9 0a00
 0002 0303 0303 6365 6e74 6563 796f  75
```

3. View the configured mirror-to-cpu buffer size

```
DUT1# show monitor cpu packet buffer
--------------------show packet buffer size ---------------------
The mirror-to-cpu packet buffer size of user set is: 100
```

4. View the configured traffic-limit of mirror-to-cpu messages transmitted up to cpu

```
DUT1# show cpu traffic-limit | include mirror-to-cpu
mirror-to-cpu             128          0
```

5. View the stored file of mirror-to-cpu messages

```
DUT1# ls flash:/mirror
Directory of flash:/mirror


total 8
```

```
-rw-r-----  1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----  1 2568 Jan  3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
14.8T bytes total (7.9T bytes free)
DUT1# more flash:/mirror/ MirCpuPkt-2017-01-03-11-41-33.txt
sequence  srcPort
1         eth-0-1
++++++++1483443444:648884
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
--------
sequence  srcPort
2         eth-0-1
++++++++1483443445:546440
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
```

6. Can be opened with wireshark after being converted into a pcap file.

```
DUT1#ls flash:/mirror
Directory of flash:/mirror

total 12
-rw-r-----  1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----  1 2568 Jan  3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
-rw-r--r--  1  704 Jan  3 13:07 test.pcap
14.8T bytes total (7.9T bytes free)
```

7. View mirror-to-cpu capture strategy

```
DUT1# show monitor cpu capture strategy
The capture strategy of cpu mirror is: replace (add new packet and remove oldest
 packet when buffer is full)
```

3.7 CPU Mirror Source Configuration

3.7.1 Introduction

Users can configure CPU as the mirror source in the ingress direction, egress direction and both way. If it is needed to mirror messages to or from the cpu to a port, CPU mirror source configuration can be enabled. It's worth noting that the mirrored messages precede cpu-traffic-limit. Only session 1 allows cpu mirror source configuration at this time.

3.7.2 Configuration

1. Set CPU as the mirror source port in configuration mode:

Switch# configure terminal	Enter configuration mode

Switch(config)# monitor session 1 source cpu both	Configure cpu as the mirror source of session 1 in both way
Switch(config)# monitor session 1 destination interface eth-0-1	Configure physical port eth-0-1 as the mirror destination port of session 1
Switch# exit	Exit global configuration mode

3.7.3 Command Validation

Configure cpu as the mirror source of session 1, and eth-0-1 as the mirror destination port of session 1

```
DUT1# show monitor session 1
Session  1
----------
Status              : Valid
Type                : Cpu Session
Source Ports        :
  Receive Only      :
  Transmit Only     :
  Both              : cpu
Source VLANs        :
  Receive Only      :
  Transmit Only     :
  Both              :
Destination Port    : eth-0-1
```

3.8 Device Management Configuration

3.8.1 Introduction

Users can manage switches via the management port. Switches are provided with two types of management port: Ethernet port and serial port.

3.8.2 Configure Serial Port

I. Configuration

The default serial port configuration of switches is as below:

- Baud rate: **115200**
- Data bit: 8
- Stop bit: 1
- No odd-even check

Before configuring a switch, please make sure that the the serial port of the switch is linked to the serial port of a PC or other terminals and the configuration of the serial port of the PC or

terminals is consistent with the default configuration of the switch. You can change the configuration parameters of the serial port after logging in the switch.

Switch# configure terminal	Enter global configuration mode
Switch(config)# line console 0	Enter serial port configuration mode
Switch(config-line)# speed 19200	Set baud rate of serial port

II. Command validation

The serial port parameters will be changed by completing the above configuration, where the PC or terminals become unable to configure the switch via the serial port. To reconnect the switch for making configuration, the serial port attributes of the PC or terminal must be changed, and the baud rate must be changed from 115200 to 19200.

3.8.3 Configure Out-of-band Management Interface

To configure switches via an out-of-band management interface, the management IP address of the out-of-band management port must be configured via the serial port first.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# management ip address A.B.C.D/M	Configure switch management IPv4 address A.B.C.D – management IPv4 address M - subnet mask
Switch(config)# management ipv6 address A:B::C/M	Configure switch management IPv6 address A:B::C – management IPv6 address M - subnet mask
Switch(config)# exit	Exit
Switch# show management ip address	Validate the set management IPv4 address
Switch# show management ipv6 address	Validate the set management IPv6 address

II. Command validation

After the configuration above is completed, the configured IP address can be viewed by entering “show management ip address” or “show management ipv6 address” in the command line. The IP address also can be validated executing the ping A B C D instruction via the PC.

Switch# show management ip address

```
 Management IP address is:  A.B.C.D/M
 Gateway: 0.0.0.0
Switch # show management ipv6 address
 Management IPv6 address is:  2001:1000::1/96
```

Gateway: ::

3.8.4 Configure Thermal Management

Switches support temperature alarm management function. Users can set three temperature thresholds: low temperature alarm threshold, high temperature alarm threshold, and superhigh temperature power-off protection threshold. Switches will automatically generate an alarm message if the temperature is below the low temperature alarm threshold or above the high temperature alarm threshold. Switches will automatically cut power for system protection if the temperature is above the superhigh temperature power-off protection threshold.

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# temperature 5 70 90	Set new temperature thresholds in celsius degree
Switch(config)# exit	Exit
Switch#show environment	Validate the set temperature thresholds

II. Command validation

Switch# show environment

Sensor status (Degree Centigrade):

Index Temperature Lower_alarm Upper_alarm Critical_limit

1 50 5 75 90

3.8.5 Configure Fan Management

Switches support automatic fan management. Switches will automatically generate an alarm message if the fan disk is not in place or the fan breaks down. If the fan disk supports fan speed adjustment, switches will automatically adjust the fan speed to the internal real-time temperature value of the system. There are three temperature thresholds provided for switch fan speed adjustment: Tlow=50 degree, Thigh=65 degree, Tcrit=80 degree. The fan will stop if the real-time temperature is below Tlow; the fan will rotate at its 30% speed if the real-time temperature is not lower than Tlow and below Thigh; the fan will rotate at its 70% speed if the real-time temperature is not lower than Thigh and below Tcrit; the fan will rotate at the full speed if the real-time temperature is equal to and above Tcrit. Besides, automatic fan adjustment supports a temperature hysteresis (Thyst) of 2 degree. If the temperature turns above a threshold to raise the fan speed by a level and then drops below the threshold, the fan speed will not go back to the previous level immediately until the real-time temperature is lower than the threshold by Thyst (2 degree). Example:

The current temperature is 58 Celsius degree and the fan speed is 30%; (Tlow<58<Thigh).

The fan speed automatically turns to 70% as the temperature rises to 65 Celsius degree; (Thigh==65)

The fan speed remains at 70% even if the temperature drops to 63 Celsius degree; (Thigh-Tyst==63)

The fan speed drops to 30% when the temperature drops to 62 Celsius degree; (62<Thigh-Thyst)

I. Configuration

Tlow, Thigh, Trict and Thyst and the corresponding fan speeds are system-defined data, and don't support user adjustment.

II. Command validation

Switch# show environment

```
Fan tray status:
Index    Status
1        PRESENT
FanIndex   Status SpeedRate Mode
1-1        OK     30%     Auto
1-2        OK     30%     Auto
1-3        OK     30%     Auto
1-4        OK     30%     Auto
-------------------------------------------------------------
```

3.8.6 Configure Power Management

Switches support automatic power management. Switches will automatically generate an alarm message if a power supply (dual power mode) or power supply fan fails. Switches also will generate an alarm message at the time of unplugging power module.

I. Command validation

Users can utilize command line instructions to view the power running state

Switch# show environment

```
-------------------------------------------------------------
Power status:
Index    Status   Power    Type     Fans     Control
1        PRESENT  OK       AC       -        -
2        ABSENT   -        -        -        -
3        PRESENT  OK       DC(PoE)  -        -
-------------------------------------------------------------
```

3.8.7 Configure Optical Transceiver Module

Switches support the management over basic information and diagnostic information of optical transceiver module. The basic information includes optical transceiver module type, manufacturer name, serial number, product number and the supported optical wavelength and link length. The diagnostic information includes real-time temperature, voltage, current, transmitted optical power and received optical power of optical transceiver module and the manufacturer-predefined normal working ranges, alerting thresholds and warning thresholds corresponding to the above information. Switches will automatically generate a notice or alarm

message if the optical transceiver module unplugging or the real-time information goes beyond the normal working range.

I. Command validation

Users can utilize command line instructions to view the power running state

Switch# show transceiver detail

```
Port eth-1-2 transceiver info:
Transceiver Type: 10G Base-SR
Transceiver Vendor Name : OEM
Transceiver PN          : SFP-10GB-SR
Transceiver S/N         : 201033PST1077C
Transceiver Output Wavelength: 850 nm
Supported Link Type and Length:
     Link Length for 50/125um multi-mode fiber: 80 m
     Link Length for 62.5/125um multi-mode fiber: 30 m
-------------------------------------------------------------------------------
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
The threshold values are calibrated.
-------------------------------------------------------------------------------
          High Alarm   High Warn   Low Warn    Low Alarm
Temperature   Threshold    Threshold    Threshold    Threshold
Port  (Celsius)     (Celsius)    (Celsius)    (Celsius)     (Celsius)
--------- ------------------  ----------  ----------  ----------  ----------
eth-1-2  25.92      95.00        90.00     -20.00       -25.00
-------------------------------------------------------------------------------------------------------
              High Alarm   High Warn   Low Warn    Low Alarm
      Voltage     Threshold    Threshold   Threshold    Threshold
Port     (Volts)     (Volts)      (Volts)     (Volts)      (Volts)
--------- ---------------- ---------------  ---------------  ---------------  ---------------
eth-1-2   3.32       3.80        3.70       2.90         2.80
-------------------------------------------------------------------------------------------------------
               High Alarm   High Warn   Low Warn    Low Alarm
       Current     Threshold    Threshold   Threshold    Threshold
Port   (milliamperes)  (mA)        (mA)       (mA)       (mA)
--------- ------------------  ---------------  ---------------  -----------------  -------------
eth-1-2    6.41       20.00      18.00      1.00          0.50
-------------------------------------------------------------------------------------------------------
       Optical      High Alarm   High Warn   Low Warn    Low Alarm
    Transmit Power   Threshold    Threshold    Threshold    Threshold
Port   (dBm)        (dBm)       (dBm)       (dBm)       (dBm)
--------- ------------------  ---------------  ----------------  -----------------  ----------------
eth-1-2    -2.41       2.01       1.00        -6.99        -7.96
-------------------------------------------------------------------------------------------------------
       Optical      High Alarm   High Warn    Low Warn    Low Alarm
    Receive Power    Threshold    Threshold    Threshold    Threshold
Port    (dBm)        (dBm)       (dBm)       (dBm)       (dBm)
--------- ------------------  ---------------  ----------------  ----------------  ----------------
eth-1-2     -12     -    1.00       0.00       -19.00     -20.00
-------------------------------------------------------------------------------------------------------
```

3.8.8 Update Bootrom Program

Switches support online update of Bootrom program, which will take effect after rebooting.

I. Configuration

Switch# copy mgmt-if tftp://10.10.29.160/ bootrom.bin flash:/boot/	Copy Bootrom program from TFTP server to a local flash storage medium
Switch# configure termina	Enter global configuration mode
Switch(config)# update bootrom flash:/boot/bootrom.bin	Update the designated Bootrom program
Switch(config)# exit	Exit
Switch# reboot	Reboot

II. Command validation

After completing the above configuration and rebooting, you can view the version number of the current Bootrom of the system.

```
Switch# show version
……
EPLD Version is 1
BootRom Version is 3.0.2
```

3.8.9 Update EPLD Program

Switches support online update of EPLD program. Power cut and reboot are required after update is completed, otherwise the system cannot work normally.

I. Configuration

Switch# copy mgmt-if tftp://10.10.29.160/ vme_v1.0 flash:/boot/ vme_v1.0	Copy EPLD program from TFTP server to a local flash storage medium
Switch# configure termina	Enter global configuration mode
Switch(config)# update epld flash:/boot/ vme_v1.0	Update the designated EPLD Program
Switch(config)# exit	Exit
Switch# reboot	Reboot

II. Command validation

After completing the above configuration and rebooting, you can view the version number of the current EPLD of the system

Switch# show version

……
EPLD Version is 1
BootRom Version is 3.0.2

3.9 Bootrom Configuration

3.9.1 Introduction

The main function of U-boot is to simply initialize the board and load system mirror on startup. In U-boot mode, you can utilize some essential commands.

U-boot can load system mirror from TFTP server and a hard disk, such as flash. If you are booting the system from TFTP server, you can configure the IP address of the local device and the designated TFTP server.

3.9.2 Load A Mirror from TFTP Server

I. Configuration

Step 1 Load a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server, as follows.

bootrom:> setenv bootcmd boot_tftp OS-ms-v3.1.9.it.r.bin	Load a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server
bootrom:> saveenv	Save the configuration locally
bootrom:> reset	Reset the board

Step 2 Load a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server without password, as follows.

bootrom:> setenv bootcmd boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	Load a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server without password
bootrom:> saveenv	Save the configuration locally
bootrom:> reset	Reset the board

Step 3 Directly reset the board after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server, as follows.

bootrom:> boot_tftp OS-ms-v3.1.9.it.r.bin	Directly reset the board after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server

Step 4 Directly reset the board after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server without password

bootrom:> boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	Directly reset the board after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from TFTP server without password

II. Command validation

You can validate the configuration details after configuring the above commands.

```
bootrom:> reset
……..
TFTP from server 10.10.29.160; our IP address is 10.10.29.118
Filename 'OS-ms-v3.1.9.it.r.bin'.
Load address: 0xaa00000
Loading: octeth0: Up 100 Mbps Full duplex (port  0)
#################################################################
      ####################
done
Bytes transferred = 12314539 (bbe7ab hex), 1829 Kbytes/sec
```

3.9.3 Load A Mirror from Flash

I. Configuration

Step 1 Load a mirror OS-ms-v3.1.9.it.r.bin startup system from flash, as follows.

bootrom:> setenv bootcmd boot_flash OS-ms-v3.1.9.it.r.bin	Load a mirror OS-ms-v3.1.9.it.r.bin startup system from flash
bootrom:> saveenv	Save the configuration locally
bootrom:> reset	Reset the board

Step 2 Load a mirror OS-ms-v3.1.9.it.r.bin startup system from flash and will revert the default login password configuration of the system, as follows.

bootrom:> setenv bootcmd boot_flash_nopass OS-ms-v3.1.9.it.r.bin	Load a mirror OS-ms-v3.1.9.it.r.bin startup system from flash without password
bootrom:> saveenv	Save the configuration locally.
bootrom:> reset	Reset the board
Do you want to revert to the default config file ? [Y|N|E]:Y	Y: Revert the default configuration file N: Revert the default login password configuration only E: Exit the settings

Step 3 Directly reset the system after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from flash, as follows.

bootrom:> boot_flash OS-ms-v3.1.9.it.r.bin	Directly reset the system after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from flash

Step 4 Directly reset the system after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from flash and will revert the default login password configuration of the system, as follows.

bootrom:> boot_flash_nopass OS-ms-v3.1.9.it.r.bin	Directly reset the system after loading a mirror OS-ms-v3.1.9.it.r.bin startup system from flash without password
Do you want to revert to the default config file ? [Y|N|E]:Y	Y: Revert the default configuration file N: Revert the default login password configuration only E: Exit the settings

II. Command validation

You can validate the configuration details after configuring the above commands.

bootrom:> reset

```
……
Do you want to  revert  to the default config file ? [Y|N|E]:Y
### JFFS2 loading '/boot/OS-ms-v3.1.9.it.r.bin' to 0xaa00000
Scanning JFFS2 FS: . done.
### JFFS2 load complete: 12314539 bytes loaded to 0xaa00000
## Booting image at 0aa00000 ...
  Verifying Checksum ... OK
  Uncompressing Kernel Image ... OK
……
```

3.9.4 Configure Boot IP

I. Configuration

Step 1 Configure local device IP, as follows.

bootrom:> setenv ipaddr 10.10.29.101	Set local device IP
bootrom:> saveenv	Save the configuration locally

Step 2 Assign TFTP server IP, as follows.

bootrom:> setenv serverip 10.10.29.160	Assign TFTP server IP
bootrom:> saveenv	Save the configuration locally

II. Command validation

You can validate the configuration details after configuring the above commands.

bootrom:> printenv

```
printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
……
stderr=serial
ipaddr=10.10.29.101
ipserver=10.10.29.160
Environment size: 856/2044 bytes
```

3.9.5 Online Update Bootrom

I. Configuration

bootrom:> upgrade_uboot bootrom.bin	Online update Bootrom from TFTP server

II. Command validation

You can validate the configuration details after configuring the above commands.

bootrom:> version

```
version
Bootrom 3.0.3 (Development build) (Build time: Aug  4 2011 - 11:47:06)
```

3.9.6 Set Bootrom Gateway

I. Configuration

Step 1 Configure local device gateway, as follows.

bootrom:> setenv gatewayip 10.10.37.1	Set the gateway address of switch Bootrom
bootrom:> saveenv	Save the configuration locally

Step 2 Configure the subnet mask of the local device, as follows.

bootrom:> setenv netmask 255.255.255.0	Set the subnet mask

bootrom:> saveenv	Save the configuration locally

II. Command validation

You can validate the configuration details after configuring the above commands:

bootrom:> printenv

```
printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
……
stderr=serial
gatewayip=10.10.38.1
netmask=255.255.255.0
Environment size: 856/2044 bytes
```

3.10 Bootup Diagnostics Configuration

3.10.1 Introduction

Bootup diagnostics can facilitate users diagnosing the workability of hardware components of switches after reboot. The diagnostic items include: EPLD, EEPROM, PHY, MAC, and so much more.

3.10.2 Configuration

The table below shows the flow of configuring bootup diagnostics.

Switch# configure terminal	Enter configuration mode
Switch(config)# diagnostic bootup level minimal	Set diagnostic level as minimal
Switch(config)# exit	Exit diagnostic mode
Switch# show diagnostic bootup level	Check if the diagnostic level is correctly configured
Switch# reboot	Reboot

3.10.3 Command Validation

The example demonstrates how to view the results of bootup diagnostics

Switch# show diagnostic bootup result detail

```
#########################################################
Item Name                Attribute Result Time(usec)
1   EPLD TEST             C         Pass   57
```

2	EEPROM0 TEST	C	Pass	101262
3	PHY TEST	C	Pass	1161
4	FAN TEST	C	Pass	4668
5	SENSOR TEST	C	Pass	5472
6	PSU TEST	C	Pass	1370
7	L2 UCAST FUNC TEST	C	Pass	40126

3.11 Bootstrap Configuration

3.11.1 Introduction

Bootstrap is a method for intelligent initialization configuration. With the Bootstrap function enabled, switches will start downloading a configuration file or image file from tftp server if no startup-config.conf file is found or the bootstrap function toggle is disabled. If it is needed to download image files of different versions, it is needed to to reboot the system.

It's worth noting that the image file and configuration file are downloaded controlling a switch via a python script file. Switches will locate the desired files to download from the python script file. The script file's name is bootstrap.py, which must be configured as needed in advance. The required information is as below:

```
options = {
  # tftp server ip
  "hostname": "192.168.1.254",

  # new target system image name
  "target_system_image": "XXXXXX.bin",

  # new target system image md5sum
  "image_md5sum": "f7ea31029b33d3f77d7c2156a814e6d7",

  # tftp server config path
  #config_sw=1 get config, config_sw=0 no get config
  "config_sw": 1,
  "config_path": "/tftpboot/",

  # tftp server target system image path
  "target_image_path": "/tftpboot/",
```

```
    "destination_path": "/mnt/flash/boot/",
}
```

The part in red must be set by users,

Hostname: tftp server ip address.

Target_system_image: File name of the version to be updated.

Image_md5sum: MD 5 value of the image file. Null means the image is not subject to MD5 authentication. Otherwise, the image will be subject to MD5 authentication.

Config_sw: Toggle for downloading a configuration file. 1 means downloading, and 2 means not downloading.

Config_path: Path for downloading a configuration file. Please note that a configuration file name is not required here.

Config_path: Path for downloading an image file. Similarly, an image file name is not required here.

After the python file is configured, image downloading will not be performed if the target_system_image in the python script is consistent with the version in the switch, and only configuration file downloading and configuration updating will be performed. In the case of inconsistency, an image file will be downloaded first, and reboot will be conducted after updating the image version, and configuration downloading and updating will be conducted subsequently.

Note: If it is needed to reuse the configuration file after completing an update of configuration, the /mnt/flash/boot/increment-config.cfg file must be deleted manually, then the bootstrap function will be executed. In the case of bootup without a startup-config.conf file (namely bootup with empty configuration), the increment-config.cfg file will be automatically deleted.

3.11.2 Topology

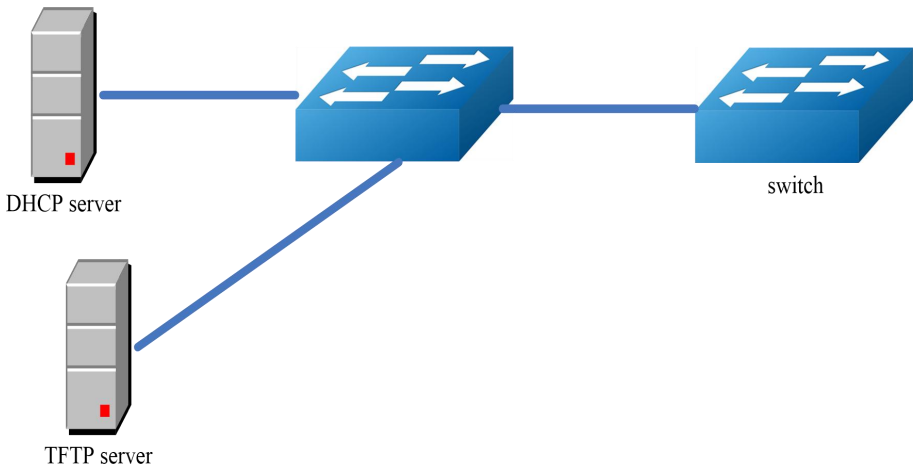


Figure 1-3 Bootstrap Topology

The figure above shows the network topology of testing Bootstrap, where two switches and two PCs are needed to construct the testing environment. The switches are provided for enabling the Bootstrap function. It’s worth noting that the TFTP server address provided by DHCP server in the figure above must be connectable directly or routable to the switch.

3.11.3 Configuration

Configure Bootstrap

Switch#configure terminal	Enter global configuration mode
Switch(config)#bootstrap enable	Set enabling Bootstrap
Switch(config)# exit	Exit interface configuration mode

Since the Bootstrap function is disabled by default, the switch will start the Bootstrap process on startup only if there is no startup-config.conf file or the bootstrap toggle is turned on. The startup-config.conf file also can be deleted manually, so that Bootstrap will work on startup next time.

The concrete configuration steps are as below:

1. Configure DHCP server, and option 66: tftp-server name and option67: bootfile-name must be set; the option 66 field must be set in the format of IP address, such as 10.0.0.1 or ERROR! Invalid hyperlink reference. The “ERROR! Invalid hyperlink reference.” 67 field is the path name for downloading the python script file, such as /tftpboot/boostrap.py.

2. Download a script file bootstrap.py from tftp server via the information of the DHCP server end, the content of the python script must be predefined according to customer's requirements, and put the image file and configuration file to be updated in the tftp server corresponding to the python script.

The image file name must be consistent with the target_system_image filled in the python script file.

Format of the configuration file name: device SN number.cfg, such as U50R9390071.cfg

or device MAC address.cfg, such as 6cec5a084e93.cfg

Note: Device SN number is case sensitive, and device MAC address refers to device management MAC address and must be lowercase. (Can be viewed via command "show management interface")

3. Make sure the switch has no startup-config.conf file or the bootstrap toggle is turned on.

Note: If there is a startup-config.conf file but the bootstrap toggle is turned on, the management port must be configured as DHCP mode and then reboot. This limit doesn't apply to startup with empty configuration.

4. Boot or reboot the system.

3.11.4 Command Validation

Check Bootstrap configuration

Switch# show running-config

```
!
bootstrap enable
!
line con 0
 no line-password
 no login
line vty 0 7
 exec-timeout 35791 0
 privilege level 4
 no line-password
 no login
!
end
```

3.12 Reboot Information

3.12.1 Introduction

Centec switch supports showing reboot information, and the reboot information will show the reason for board reboot, including power failure reboot, manual reboot, and so much more. Users can clear the reboot information via one command.

3.12.2 Command Validation

The reboot information can be displayed by running the command below

```
Switch# show reboot-info
Times     Reboot Type     Reboot Time(DST)
1         MANUAL          2000/01/01 01:21:35
2         MANUAL          2000/01/01 02:07:52
3         MANUAL          2000/01/01 2:24:59 AM
4         MANUAL          2000/01/01 3:28:58 AM
5         MANUAL          2000/01/01 3:43:02 AM
6         MANUAL          2000/01/01 3:49:51 AM
7         MANUAL          2000/01/01 4:01:23 AM
8         MANUAL          2000/01/01 4:42:40 AM
9         MANUAL          2000/01/01 4:49:27 AM
10        MANUAL          2000/01/01 20:59:20
```

The reboot information can be cleared via the command below

```
Switch(config)# reset reboot-info
```

3.12.3 Note

Only 10 reboot records will be displayed at most by running this command. For more reboot records, please access the file: flash:/reboot-info/reboot_info.log

The description of show results is as below:

Reboot type	Description
POWER	Power failure reboot
MANUAL	Manual reboot/reload under the system
HIGH-TMPR	High temperature reboot
BHMDOG	BHM dog reboot, applied for monitoring functional modules of the system
LMDOG	LCM dog reboot, applied for monitoring LC
SCHEDULE	Scheduled reboot
SNMP-RELOAD	SNMP reboot
HALFAIL	HAGT and HSRV failure reboot, requiring stack function enabled
ABNORMAL	Abnormal system abnormal, including reboot under shell
CTCINTR	Key-pressing reboot
LCATTACH	Outlier LC matching reboot
OTHER	Other reboot

4 Network Management Configuration Guide

4.1 Network Diagnostics Configuration

4.1.1 Introduction

Ping is a computer network management tool for testing the reachability of a host via IP protocol and measuring the source-to-destination round trip time. Its name is derived from a term of active sonar.

Ping is realized by transmitting an ICMP echo request to the destination host and waiting for an ICMP response. In the operation process, the round trip time (from sending to receiving to responding) will be measured and all packet dropouts will be recorded. All received messages will be displayed in the results as a statistical summary, including minimum, maximum and mean round-trip time, and the mean standard values of deviation will be printed sometimes.

Traceroute is a tool for measuring routing and message transfer time on IP network.

Traceroute transmits an ICMP sequence message to the destination host and trace the intermediate router via TTL parameters. The intermediate router reduces the transferred message TTL parameter values. The messages will be discarded if the TTL value is 0, and an ICMP error message (ICMP Timer Exceeded) will be returned to the source.

4.1.2 Configuration

IP Address of Internal Ping Interfaces

DUT# ping 10.10.29.247	IPv4 address 10.10.29.247 of the internal Ping interface
DUT# ping ipv6 2001:1000::1	IPv6 address IP 2001:1000::1 of the internal Ping interface

Ping Management IP

DUT# ping mgmt-if 10.10.29.247	Ping out-of-band management IPv4 address 10.10.29.247
DUT# ping mgmt-if ipv6 2001:1000::1	Ping out-of-band management IPv6 address 2001:1000::1

IP of Ping VRF Instance

DUT# ping vrf vrf1 10.10.10.1	IP 10.10.10.1 of Ping VRF instance

Traceroute Internal Interface IP

DUT# traceroute 1.1.1.2	Traceroute internal interface IP 1.1.1.2
Switch# traceroute ipv6 2001:1000::1	Traceroute internal interface IP 2001:1000::1

4.1.3 Command Validation

```
Switch # ping mgmt-if 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
64 bytes from 192.168.100.101: icmp_seq=0 ttl=64 time=0.092 ms
64 bytes from 192.168.100.101: icmp_seq=1 ttl=64 time=0.081 ms
64 bytes from 192.168.100.101: icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from 192.168.100.101: icmp_seq=3 ttl=64 time=0.071 ms
64 bytes from 192.168.100.101: icmp_seq=4 ttl=64 time=1.10 ms
--- 192.168.100.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.071/0.408/1.104/0.421 ms, pipe 2
Switch# traceroute 1.1.1.2
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
 1  1.1.1.2 (1.1.1.2)  112.465 ms  102.257 ms  131.948 ms
Switch # ping mgmt-if ipv6 2001:1000::1
PING 2001:1000::1(2001:1000::1) 56 data bytes
64 bytes from 2001:1000::1: icmp_seq=1 ttl=64 time=0.291 ms
64 bytes from 2001:1000::1: icmp_seq=2 ttl=64 time=0.262 ms
64 bytes from 2001:1000::1: icmp_seq=3 ttl=64 time=0.264 ms
64 bytes from 2001:1000::1: icmp_seq=4 ttl=64 time=0.270 ms
64 bytes from 2001:1000::1: icmp_seq=5 ttl=64 time=0.274 ms
--- 2001:1000::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.262/0.272/0.291/0.014 ms
Switch #
```

4.2 NTP Configuration

4.2.1 Introduction

NTP is a hierarchical time distribution system with redundant capacity. NTP is for measuring inner network delay and delay due to running its algorithm on devices. With such technology, NTP can realize time synchronization across devices within an LAN to millisecond level and

time synchronization across devices in the WAN to hundred millisecond level. The hierachical feature of NTP time distribution tree enables users to select a desired accuracy from a specific level (hierarchy). A time server placed at the high end (low-level) of the tree provides high-precision UTC standard time.

A host can act as a time server to provide time regarded correct by itself to other hosts. A host also can act as a client to transmit a request of time synchronization to the server. Hosts also can act as both clients and server, because these hosts are on the same link, and a correct time is forwarded from one host to another. As part of the link, a host acquires a correct time from another host acting as a time server as a client first. Then it acts as a time server of time synchronization for other hosts.

Please confirm the NTP server has enabled NTP service before configuring the NTP client.

4.2.2 Configuration

I. Configure interface vlan10

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 10	Add VLAN 10 into database
Switch(config-vlan)# exit	Exit VLAN configuration mode
Switch(config)# interface eth-0-26	Enter interface configuration mode
Switch(config-if)# switch access vlan 10	Add the interface into vlan 10
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface vlan10	Enter VLAN configuration mode
Switch(config-if)# ip address 6.6.6.5/24	Set IP address
Switch(config-if)# exit	Exit VLAN configuration mode

II. Configure NTP client

Switch(config)# ntp key 1 serverkey	Enable trustedkey
Switch(config)# ntp server 6.6.6.6 key 1	Configure IP address of NTP server
Switch(config)# ntp authentication enable	Enable authentication
Switch(config)# ntp trustedkey 1	Once authentication is enabled, the client switch transmits a time-of-day request to the trusted NTP server only
Switch(config)# ntp ace 6.6.6.6 none	Configure ntp ace

III. Configure NTP server

Step 1 Show eth1 IP address.

[root@localhost octeon]# ifconfig eth1

```
eth1      Link encap:Ethernet  HWaddr 00:08:C7:89:4B:AA
          inet addr:6.6.6.6  Bcast:6.6.6.255  Mask:255.255.255.0
          inet6 addr: fe80::208:c7ff:fe89:4baa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3453 errors:1 dropped:0 overruns:0 frame:1
          TX packets:3459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:368070 (359.4 KiB)  TX bytes:318042 (310.5 KiB)
```

Step 2 Check network connection via ping.

[root@localhost octeon]# ping 6.6.6.5

```
PING 6.6.6.5 (6.6.6.5) 56(84) bytes of data.
64 bytes from 6.6.6.5: icmp_seq=0 ttl=64 time=0.951 ms
64 bytes from 6.6.6.5: icmp_seq=1 ttl=64 time=0.811 ms
64 bytes from 6.6.6.5: icmp_seq=2 ttl=64 time=0.790 ms
```

Step 3 Configure ntp.conf.

[root@localhost octeon]# vi /etc/ntp.conf

```
server  127.127.1.0 # local clock
fudge   127.127.1.0 stratum 5
#
# Drift file.  Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then rename()'ing
# it to the file.
#
driftfile /var/lib/ntp/drift
broadcastdelay  0.008
broadcast 6.6.6.255
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
#disable auth
keys       /etc/ntp/keys
trustedkey 1
```

Step 4 Configure keys.

[root@localhost octeon]# vi /etc/ntp/keys

```
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
```

```
# will have to be removed as well.
#
1 M serverkey
```

Step 5 Boot the ntpd server.

```
[root@localhost octeon]# ntpd
```

4.2.3 Command Validation

```
Switch# show ntp
Current NTP configuration:
==========================================================
NTP access control list:
  6.6.6.6 none
Unicast peer:
Unicast server:
  6.6.6.6 key 1
Authentication: enabled
Local reference clock:
Switch# show ntp status
Current NTP status:
==========================================================
clock is synchronized
stratum:        7
reference clock: 6.6.6.6
frequency:       17.365 ppm
precision:       2**20
reference time:  d14797dd.70b196a2  ( 1:54:37.440 UTC   Thu Apr  7 2011)
root delay:      0.787 ms
root dispersion: 23.993 ms
peer dispersion: 57.717 ms
clock offset:    -0.231 ms
stability:       6.222 ppm
Switch# show ntp associations
Current NTP associations:
  remote          refid      st   when poll reach   delay   offset  disp
==========================================================================
*6.6.6.6         127.127.1.0    6   50  128   37      0.778   -0.234  71.945
synchronized, + candidate, # selected, x falsetick, . excess, - outlier
```

Note

Users can disable auth in the ntp.conf file and disable ntp authentication on the device if not wanting to turn on the authentication option.

The startum number of the NTP server end must be less than that of the current client end.

4.3 Phy Loopback Management

4.3.1 Introduction

Phy loopback is a private module for realizing loopback function of the physical layer. It includes loopbacks of two levels: loopbacks realized via phy hardware (including internal mode and external mode) and port-level loopbacks realized via a chip.

Phy loopback can be configured on physical port only:

- If an external phy mode is configured, all messages entering this port will be looped back.
- If an internal phy mode is configured, all messages expected to transmit from this port will be looped back to another designated port.
- If a port loopback mode is configured, all messages entering this port will be looped back, and it can be specified in this mode whether to switch MAC address between the source and destination. If MAC is switched, the chip will recalculate the CRC checksum.

4.3.2 Configure External Phy Loopback Mode

I. Topology

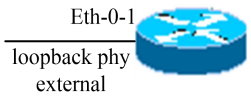


Figure 4-1 External Phy Topo

II. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# no shutdown	Configure port management up
Switch (config-if)# loopback phy external	Configure the port as external phy loopback mode
Switch(config-if)# end	Exit to privilege mode
Switch# show phy loopback	View configuration

4.3.3 Configure Internal Phy Loopback Mode

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter port configuration mode
Switch(config-if)# no shutdown	Configure port management up

Switch(config-if)# exit	Exit to global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# no shutdown	Configure port management up
Switch (config-if)# loopback phy internal eth-0-2	Configure the port as internal phy loopback mode, and assign interface 2 as destination port
Switch(config-if)# end	Exit to privilege mode
Switch# show phy loopback	View configuration

4.3.4 Configure Port Level Loopback Mode

I. Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# no shutdown	Configure port management up
Switch (config-if)# loopback port mac-address swap	Configure the port as port level loopback mode, and specify MAC switching between the source and destination
Switch(config-if)# end	Exit to privilege mode
Switch# show phy loopback	View configuration

4.3.5 Command Validation

Switch# show phy loopback

```
Interface  Type      DestIntf   SwapMac
-----------------------------------------------
eth-0-1    external  -          -
-----------------------------------------------
```

4.3.6 L2 Ping Configuration

L2 ping is a tool for checking the connectivity between switches. IP ping on Window and Linux is realized via ICMP protocol and works on layer3 network, while L2 ping works on layer2 network.

Once the system sends an L2 Ping request, the protocol message tagged with ether type 0x9009 will enter layer2 network to the designated destination port on the opposite end, and the opposite system will respond to the L2 ping request if L2 pin response is enabled on the destination port.

I. Configuration

switch2

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-2	Enter port configuration mode
Switch2(config-if)# no shutdown	Configure port management up
Switch2 (config-if)# l2 ping response enable	Enable L2 ping response
Switch2(config-if)# end	Exit to privilege mode

switch1

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# interface eth-0-1	Enter port configuration mode
Switch1(config-if)# no shutdown	Configure port management up
Switch1(config-if)# end	Exit to privilege mode
Switch1# l2 ping 001e.0808.58f1 interface eth-0-1 count 10 interval 1000 timeout 2000	001e.0808.58f1 is the interface address of the opposite interface eth-0-2 Users can specify ping count, interval and timeout

II. Command validation

Switch1# l2 ping 001e.0808.58f1 interface eth-0-9 count 10 interval 1000 timeout 2000

Sending 10 L2 ping message(s):
64 bytes from 001e.0808.58f1: sequence = 0, time = 10ms
64 bytes from 001e.0808.58f1: sequence = 1, time = 15ms
64 bytes from 001e.0808.58f1: sequence = 2, time = 13ms
64 bytes from 001e.0808.58f1: sequence = 3, time = 12ms
64 bytes from 001e.0808.58f1: sequence = 4, time = 20ms
64 bytes from 001e.0808.58f1: sequence = 5, time = 21ms
64 bytes from 001e.0808.58f1: sequence = 6, time = 12ms
64 bytes from 001e.0808.58f1: sequence = 7, time = 16ms
64 bytes from 001e.0808.58f1: sequence = 8, time = 14ms
64 bytes from 001e.0808.58f1: sequence = 9, time = 17ms
L2 ping completed.
---
10 packet(s) transmitted, 10 received, 0 % packet loss

4.4 RMON Management

4.4.1 Introduction

RMON is a monitoring specification stipulated by IETF (Internet Engineering Task Force) that allows switching network monitoring data between various network agents and console systems. Users can monitor data traffic flowing through the switches in the network with the aid of RMON and SNMP (Simple Network Management Protocol) agent of switches. RMON is a standard monitoring specification that defines a set of statistics for providing comprehensive network fault diagnosis, planning and performance optimization information together with RMON-compatible console system or network probes.

4.4.2 Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# rmon collection stats 1 owner test	Create a piece of statistics. The statistics ID is 1, and it is for recording interface statistics
Switch(config-if)# rmon collection history 1 buckets 100 interval 1000 owner test	Create a statistics history numbered 1 to record statistical value at an interval of 1000 seconds and retain 100 times
Switch(config-if)# exit	Exit interface mode
Switch(config)# rmon event 1 log trap public description test_event owner test	Create an event with an ID of 1. The system will transmit log and trap if the event is triggered
Switch(config)# rmon alarm 1 etherStatsEntry.6.1 interval 1000 delta rising-threshold 1000 event 1 falling-threshold 1 event 1 owner test	Create an alarm to count ETHERSTATSBROADCASTPKTS value at an interval of 1000 seconds, and event 1 will be triggered if the value is above 1000 or below 1

4.4.3 Command Validation

Switch# show rmon statistics

```
Rmon collection index 1
    Statistics ifindex = 1, Owner: test
    Input packets 0, octets 0, dropped 0
    Broadcast packets 0, multicast packets 0, CRC alignment errors 0, collisions 0
    Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
    # of packets received of length (in octets):
    64: 0,  65-127: 0, 128-255: 0
    256-511: 0,  512-1023: 0, 1024-max: 0
```

Switch# show rmon history

History index = 1
Data source ifindex = 1
Buckets requested = 100
Buckets granted = 100
Interval = 1000
Owner: test

Switch# show rmon event

Event Index = 1
Description: test_event
Event type Log & Trap
Event community name: public
Last Time Sent = 00:00:00
Owner: test

Switch# show rmon alarm

Alarm Index = 1
Alarm status = VALID
Alarm Interval = 1000
Alarm Type is Delta
Alarm Value = 00
Alarm Rising Threshold = 1000
Alarm Rising Event = 1
Alarm Falling Threshold = 1
Alarm Falling Event = 1
Alarm Owner is test

4.5 SNMP Network Management

4.5.1 Introduction

SNMP is a communication protocol between network management station (NMP) and agent. It specifies the standardization management framework, common communication language and corresponding security and access control mechanism for monitoring and managing devices in the network environment. SNMP allows network administrators to query equipment information, modify equipment parameter values, monitor equipment state, automatically discover network malfunction and generate reports, and so much more.

SNMP has the following technological advantages:

- Based on standard TCP/IP protocols and usually with UDP as the transport layer protocol.
- Automation network management. Network administrators can utilize the nodes of SNMP platform on the network to retrieve information, modify information, detect failures, complete fault diagnosis, make capacity planning and generate reports.
- Shield the physical discrepancies in all kinds of devices, and realize automated management of products from various vendors. SNMP only provides the most basic function library to make management tasks be relatively independent from the physical properties of the managed devices and the actual network type, so as to realize management of devices from various vendors.

- A combination of simple request-response mode with active notification mode with timeout and retransmission mechanism.
- A small variety of messages in simple format that are easy to resolute and realize.
- SNMPv3 provides an authentication and encryption security mechanism and an access control function based on users and views, which enhances the security.

4.5.2 References

SNMP is based on the following RFCs:

SNMPv1: Defined in FRC1157

SNMPv2C: Defined in FRC1901

SNMPv3: Defined in FRC2273 to 2275

4.5.3 Terms

The below briefs the entries and concepts of SNMP protocol.

Agent

Agent is an application module in network devices for maintaining the information data of the managed devices, responding to NMS requests and reporting the management data to the NMS sending requests. Agent completes query or modification action based on the request from NMS, and sends the result of the action to NMS to complete response. Meanwhile, in the case of device failure or other events, Agent will actively send a Trap message to NMS to inform of the change of device state.

Management Information Base (MIB)

Each managed resource is expressed an object, which is called managed object. MIB refers to a set of managed objects. It defines a series of properties of managed object: object name, object access permission and object data type. Every Agent has its own MIB. MIB also can be regarded an interface between NMS and Agent through which NMS can read/write every managed object in the Agent to attain the goal of device management and monitoring.

Engine ID

Refers to a unique ID of a network node.

Trap

Trap is a message actively sent by Agent to NMS for reporting some emergent critical events (such as reboot of managed device, etc.). Trap messages are classified into two types: common Trap and enterprise custom Trap. The supported common Trap of the devices include authentication, coldstart, linkdown, linkup and warmstart, and the rest messages are enterprise custom Trap. Enterprise custom Trap is generated by module. Since the amount of Trap information is usually large to consume device memory to affect device performance, users are suggested to enable the Trap feature of specific module as needed to generate relevant Trap messages.

4.5.4 Topology

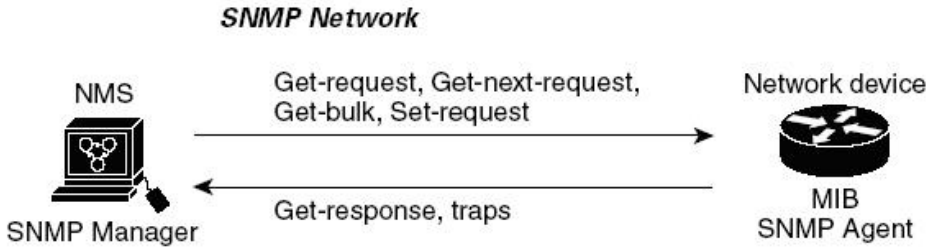


Figure 4-2 SNMP Network

4.5.5 Enable SNMP

I. Configuration

Enable SNMP service in privilege EXEC mode

Switch# configure terminal	Enter configuration mode
Switch(config)# snmp-server enable	Enable SNMP
Switch(config)# end	Exit configuration mode
Switch# show running-config	Show configuration

II. Command validation

Switch# show running-config

snmp-server enable

4.5.6 Community String Configuration

You can define the relationship between SNMP administrator and agent with SNMP community string. The behavior of community string is like a password for allowing access to agent switches. You can specify one or more community characters.

- An MIB view that definesa set of MIB objects that all given communities have access to.
- Set the read-write access permission of accessed MIB objects.

The basic read-write function of SNMP can be realized by following the steps below to complete configuring a community string on switch in the privilege EXEC mode.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# snmp-server view DUT included 1	Configure a view name “DUT” (optional)

Switch(config)# snmp-server community public read-write (view DUT)	Configure a community name "public" read-write access permission, accessible view “DUT” with an optional field bracketed
Switch(config)# end	Exit configuration mode

II. Command validation

Switch# show running-config

snmp-server enable
snmp-server view DUT included .1
snmp-server community public read-only view DUT

4.5.7 Configuration of SNMPv3 Groups, Users and Accesses

You can assign an engine ID for SNMP server, create an SNMP group with the user and setting permissions defined.

Configure SNMP on a switch in the privilege EXEC mode following the steps below.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch (config)# snmp-server engineID 8000123456	Configure engine ID
Switch(config)# snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword	Configure user name, password and authentication type
Switch(config)# snmp-server group grp1 user usr1 security-model usm	Create SNMP group
Switch(config)# snmp-server access grp1 security-model usm noauth	Set group member permissions
Switch(config)# end	Exit global mode

II. Command validation

Switch# show running-config

snmp-server engineID 8000123456
snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword
snmp-server group grp1 user usr1 security-model usm
snmp-server access grp1 security-model usm noauth

4.5.8 Configuration of SNMPv1 and SNMPv2 Notifications

Configure SNMP on a switch in the privilege EXEC mode following the steps below.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# snmp-server trap enable all	Enable all Traps
Switch(config)# snmp-server trap target-address 10.0.0.2 community public	Configure target IPv4 address and community name Public
Switch(config)# snmp-server trap target-address 2001:1000::1 community public	Configure target IPv6 address and community name Public
Switch(config)# end	Exit configuration mode

II. Command validation

Switch# show running-config

```
snmp-server trap target-address 10.0.0.2 community public
snmp-server trap target-address 2001:1000::1 community public
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

4.5.9 Configuration of SNMPv3 Notifications

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# snmp-server trap enable all	Enable all Traps
Switch(config)# snmp-server notify notif1 tag tmptag trap	Create a Trap message entry
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag	Configure target IPv4 address and community name Public
Switch(config)# snmp-server target-address t1 param p1 2001:1000::1 taglist tag1	Configure target IPv6 address and community name Public

Switch(config)# snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth	Add a user into SNMP group
Switch(config)# end	Exit configuration mode
Switch# show running-config	Check configuration

II. Command validation

Switch# show running-config

```
snmp-server notify notif1 tag tmptag trap
snmp-server target-address t1 param p1  2001:1000::1 taglist tag1
snmp-server target-address targ1 param parm1  10.0.0.2 taglist tmptag
snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

4.6 Sflow Configuration

4.6.1 Introduction

Sflow refers to Sampled Flow, and is a technology of monitoring ingress device traffic. It is applied to surveillance equipment to sample at a certain rate as per a sampling mechanism and transmit the sampling information to the monitor server. The bandwidth usage of multiple agents can be viewed on the server end.

Sflow relates to two types of sample information: statistical information of ports and header of sampled messages.

4.6.2 Terms

Sflow： Sampled flow

4.6.3 Topological Graph

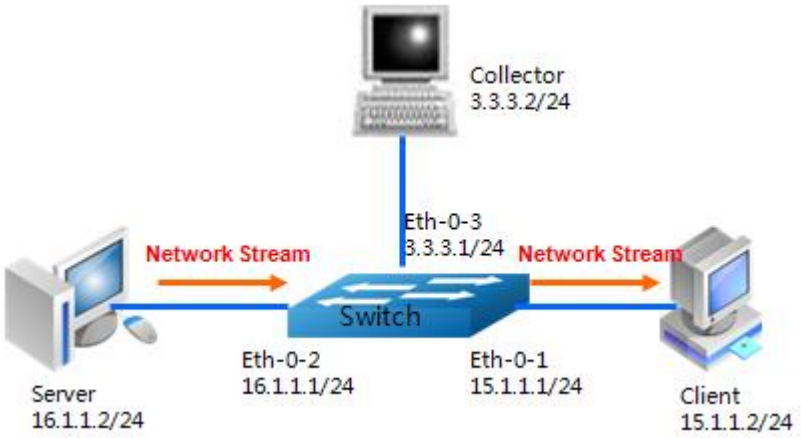


Figure 4-3 Sflow Topology

4.6.4 Configuration

Default Configuration

Feature	Default Setting
Global sflow	disabled
sflow on port	disable
Collector udp port	6343
counter interval time	20 seconds

Sflow Configuration

This section shows basic examples of configuring Sflow. All ingress messages of eth-0-1 will be sampled at a certain rate and sent to collector PC 3.3.3.2.

Switch# configure terminal	Enter configuration mode
Switch(config)# sflow enable	Globally enable Sflow
Switch(config)# sflow counter interval 20	Configure statistical-based sampling interval
Switch(config)# sflow agent ip 3.3.3.1	Configure agent address
Switch(config)# sflow collector 3.3.3.2 6342	Configure collector address
Switch(config)# sflow collector 2001:1000::1	Configure collector address

Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# sflow flow-sampling rate 8192	Configure message-based sampling rate
Switch(config-if)# sflow flow-sampling enable input	Enable message-based sampling function on the interface
Switch(config-if)# sflow counter-sampling enable	Enable statistical-based sampling function on the interface
Switch(config-if)# no switchport	Switch the interface to a layer3 port
Switch(config-if)# ip address 15.1.1.1/24	Configure interface IP address
Switch(config-if)# exit	Exit to config mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Switch to a layer3 interface
Switch(config-if)# ip address 16.1.1.1/24	Configure interface IP address
Switch(config-if)# exit	Exit to config mode
Switch(config)# interface eth-0-3	Enter interface mode
Switch(config-if)# no switchport	Switch to a layer3 interface
Switch(config-if)# ip address 3.1.1.1/24	Configure interface IP address

4.6.5 Command Validation

View Sflow configuration using the following command:

Switch# show sflow

```
sFlow Global Information:
 Agent IP address             : 2.2.2.1
 Agent IPv6 address           : 2026::2
 Counter Sampling Interval    : 20 seconds
 Collector 1:
  Address: 3.3.3.2
  Port: 6342
 Collector 2:
  Address: 2001:1000::1
  Port: 6343
sFlow Port Information:
                          Flow-Sample   Flow-Sample
 Port       Counter    Flow     Direction    Rate
 ---------------------------------------------------
 eth-0-1    Enable     Enable   Input        8192
```

4.7 LLDP Configuration

4.7.1 Introduction

LLDP (Link Layer Discovery Protocol) is a layer2 discovery protocol defined in

IEEE 802.1ab. Layer 2 Discovery allows to accurately identify interface types of devices and layer 2 information such as interconnection of devices, such as VLAN attributes and supported protocol types of port, and display the path between client, switch as well as router and application server as well as network server. Such details can facilitate rapidly fetching topological state of connected devices, configuration conflicts among devices and primary cause of failure of network inquiry.

4.7.2 Terms

LLDP: Link Layer Discovery Protocol

4.7.3 Configuration

Basic Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# lldp enable	Globally enable LLDP
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config)# no shutdown	Open the interface
Switch(config-if)# no lldp tlv 8021-org-specific vlan-name	Deselect IEEE 802.1 tlv concentration Vlan Name TLV
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890	Select and configure MED tlv concentration Location ID TLV
Switch(config-if)# lldp enable txrx	Enable LLDP on the interface and configure the mode as TXRX

Status Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# lldp timer msg-tx-interval 40	Set the transmission interval of LLDP messages as 40 seconds
Switch(config)# lldp timer tx-delay 3	Set the transmission delay of LLDP messages as 3 seconds
Switch(config)# lldp timer reinitDelay 1	Set the re-enabling delay of LLDP messages as 1 seconds

4.7.4 Command Validation

View LLDP configuration using the following command:

```
Switch# show lldp local config
LLDP global configuration:
=============================================================
LLDP function global enabled : YES
LLDP msgTxHold     : 4
LLDP msgTxInterval : 40
LLDP reinitDelay   : 1
LLDP txDelay       : 3
Switch# show lldp local config interface eth-0-9
LLDP configuration on interface eth-0-9 :
=============================================================
LLDP admin status : TXRX
Basic optional TLV Enabled:
   Port Description TLV
   System Name TLV
   System Description TLV
   System Capabilities TLV
   Management Address TLV
IEEE 802.1 TLV Enabled:
   Port Vlan ID TLV
   Port and Protocol Vlan ID TLV
   Protocol Identity TLV
IEEE 802.3 TLV Enabled:
   MAC/PHY Configuration/Status TLV
   Power Via MDI TLV
   Link Aggregation TLV
   Maximum Frame Size TLV
LLDP-MED TLV Enabled:
   Med Capabilities TLV
   Network Policy TLV
   Location Identification TLV
   Extended Power-via-MDI TLV
   Inventory TLV
Switch# show running-config
!
lldp enable
lldp timer msg-tx-interval 40
lldp timer reinit-delay 1
lldp timer tx-delay 3
。 。 。
interface eth-0-9
lldp enable txrx
 no lldp tlv 8021-org-specific vlan-name
 lldp tlv med location-id ecs-elin 1234567890
!
Switch# show lldp neighbor
Remote LLDP Information
=============================================================
Chassis ID type: Mac address
```

Chassis ID : 48:16:be:a4:d7:09
Port ID type : Interface Name
Port ID : eth-0-9
TTL : 160
Expired time: 134
…
Location Identification :
ECS ELIN: 123456789

5 Multicast Configuration Guide

5.1 IP Multicast-Routing Configuration

5.1.1 Introduction

With the continuous development of the Internet, many interactive services such as network data, voice and video information are steadily on the increase. Besides, services requiring high bandwidth and real-time data interaction performance such as emerging e-business, online meeting, online auction, video on demand and distance teaching rise gradually, which demand more in respect of information security, accountability and network bandwidth.

The situation where the efficiency of unicast and broadcast will be low if the number of users needing certain information in the network is uncertain has been changed by the emergence of the IP multicast technology. Where some users in the network need specific information, multicast information sender (namely multicast source) will send information once only and establish a tree based routing with multicast routing protocol for multicast data packets, and the transmitted information will not be copied and distributed until reaching the node as close as possible to user side.

With multicast routing protocol, multiple receivers can receive multicast data across various networks.

- IGMP (Internet Group Management Protocol) is a protocol of TCP/IP protocol family responsible for IP multicast member management. It is used to establish and maintain multicast member relationships between IP host and its direct adjacent multicast router.
- PIM (Protocol Independence Multicast) is applied between multicast routers or between multilayer switches. The unicast routing protocol routing IP multicast can be static routing, RIP, OSPF, IS-IS or BGP, multicast routing and unicast routing are protocol independent as long as unicast routing protocol can generate routing table entries. By virtue of RPF (Reverse Path Forwarding) mechanism, PIM has realized multicast information transfer in the network. To facilitate describing, the network composed with multicast routers supporting PIM protocol is called PIM multicast domain. PIM is classified into dense mode and sparse mode, and we support sparse mode only for the moment.

5.1.2 Configuration

We can support multicast routing table with a limit of 2048 entries by default.

Switch# configure terminal	Enter configuration mode

Switch(config)# ip multicast route-limit 1000	Configure maximum multicast entry limit

5.1.3 Check Configuration

Switch# show ip mroute 192.168.47.2

```
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(192.168.47.2, 238.255.0.1), uptime 00:00:03, stat expires 00:03:27
Owner PIM-SM, Flags: TF
  Incoming interface: eth-0-3
  Outgoing interface list:
    Register (1)
    eth-0-1 (1)
(192.168.47.2, 238.255.0.2), uptime 12:00:02 AM, stat expires 12:03:28 AM
Owner PIM-SM, Flags: TF
  Incoming interface: eth-0-3
  Outgoing interface list:
    Register (1)
    eth-0-2 (1)
```

5.2 IGMP Configuration

5.2.1 Introduction

The host, router and multilayer switch participating in IP multicast must have the IGMP feature. This protocol defines querier and host role:

- The querier of network devices sends query messages to a specific group in the network to discover multicast members.
- The host sends IGMP report messages (to respond to the query messages) to notify the querier that the host will join in corresponding multicast group list.
- The members of a multicast group are dynamic, and the host can join and exit at any time. No limitation is set on the position or count of multicast members.

A host can act as a member of multiple multicast groups. At the same time, members are active in the multicast groups, which can change with group and with the time. A multicast group can last a long time or briefly.

IGMP messages use the following multicast addresses:

- 224.0.0.1 as destination address (all systems in a subnet) for query by a general IGMP group.
- Group-specific IP address as destination address for an IGMP group-specific query.
- IGMP group members send Report messages to specific multicast IP addresses.
- IGMPv2 sends a message to 224.0.0.2 at the time of exiting the multicast group.

5.2.2 References

IGMP module is based on the following RFCs

- RFC 1112
- RFC 2236
- RFC 3376

5.2.3 Configuratin

Enabling IGMP is dependent on enabling multicast routing protocol. IGMP will be automatically enabled once PIM or other multicast routing protocols are enabled on the interface, and vice versa. Please note that IP multicast routing must be enabled in global mode before IGMP runs. The system supports dynamic learning IGMP group records, and configuring static IGMP group records.

Enable IGMP

Switch# configure terminal	Enter configuration mode
Switch(config)# ip multicast-routing	Enable multicast routing in global mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.10/24	Set IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface

Configure IGMP Interface Parameters

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Access interface mode
Switch(config-if)# ip igmp version 2	Set IGMP version
Switch(config-if)# ip igmp query-interval 120	Set IGMP query interval
Switch(config-if)# ip igmp query-max-response-time 12	Set maximum IGMP query response time
Switch(config-if)# ip igmp robustness-variable 3	Set IGMP robustness
Switch(config-if)# ip igmp last-member-query-count 3	Set IGMP last member query count
Switch(config-if)# ip igmp last-member-query-interval 2000	Set IGMP last member query interval

Configure Maximum IGMP Group Limit

You can globally configure the maximum IGMP group limit or configure the maximum IGMP group limit in interface mode.

Switch# configure terminal	Enter configuration mode
Switch(config)# ip igmp limit 2000	Configure the global maximum IGMP group limit
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip igmp limit 1000	Set the maximum IGMP group limit in interface mode

Configure Static IGMP Group

You can configure a static IGMP group in interface mode.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip igmp static-group 228.1.1.1	Configure Static IGMP Group

Configure IGMP Proxy

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# ip igmp proxy-service	Set the interface as upstream port of IGMP proxy
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# ip igmp mroute-proxy eth-0-1	Set eth-0-2 as the downstream port of IGMP proxy, and eth-0-1 as the upstream port of IGMP proxy

5.2.4 Check Configuration

Show IGMP Interface Information

Switch# show ip igmp interface

```
Interface eth-0-1 (Index 1)
 IGMP Inactive, Version 2 (default) proxy-service
 IGMP host version 2
 IGMP global limit is 2000
 IGMP global limit states count is currently 0
 IGMP interface limit is 1000
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP query interval is 120 seconds
 IGMP querier timeout is 366 seconds
 IGMP max query response time is 12 seconds
 Last member query response interval is 2000 milliseconds
 Group Membership interval is 372 seconds
 Last memeber query count is 3
 Robustness Variable is 3
Interface eth-0-2 (Index 2)
 IGMP Inactive, Version 2 (default)
 IGMP mroute-proxy interface is eth-0-1
 IGMP global limit is 2000
 IGMP global limit states count is currently 0
 IGMP interface limit is 16384
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Last memeber query count is 2
 Robustness Variable is 2
```

Show IGMP Group Information

Switch# show ip igmp groups

```
IGMP Connected Group Membership
Group Address   Interface       Uptime   Expires Last Reporter
228.1.1.1       eth-0-1         00:00:05 stopped  -
```

5.3 PIM-SM Configuration

5.3.1 Introduction

Protocol independent multicast sparse mode (PIM-SM) is a multicast routing protocol for connecting sparsely distributed multicast devices for collaboration.' It helps sparse network nodes save bandwidth and reduce bandwidth usage by transmitting a single flow to multiple receivers.

PIM-SM uses receivers to initiate members' IP multicast mode, which supports the shared and shortest path tree and uses the soft-state mechanism to adapt to the constantly changing network condition. It relies on unicast routing protocol for establishing and maintaining multicast routing between routers.

5.3.2 References

PIM-SM module is based on the following IETF standard:

RFC 4601

5.3.3 Terms

The concepts related to in PIM-SM protocol are briefed below:

- **Rendezvous point (RP):** RP acts as the rendezvous point of multicast in SM mode, and senders and receivers rendezvous at the RP. Every multicast router must know the RP specific to each multicast group.

  All multicast data must be registered with RP, and all receivers who need multicast data can request data by sending a JOIN message to the RP. The source registration mechanism is to inform the RP of the sources of data in the network.
- **Multicast routing information base (MRIB):** Multicast routing table is obtained based on unicast routing table. In PIM-SM, MRIB is used to determine the target of sending join/prune messages. It also provides routing metrics of destination work. These metrics will be used when sending and processing Assert messages.
- **Reverse path forwarding (RPF)**: RPF means a router for receiving data packet from Source A passing through interface IF1 will receive the data packet only if interface IF1 is the egress interface for reaching Source A. RPF uses unicast routing table to determine whether the ingress port is correct. The data packet is forwarded because the unicast routing table indicates that interface IF1 is the shortest path to Source A. Unicast routing table selects the shortest path for multicast data.
- M**ulticast tree information base (TIB)**: TIB is an information base on multicast router for storing all multicast forwarding tree information, which is built by receiving PIM join/prune messages, Assert message and IGMP message.
- **Upstream:** It is near the tree root, and the tree root may be a source or RP.
- **Downstream:** It is away from the tree root, and the tree root may be a source or RP.
- **Source-based tree:** The forwarding path of source-based tree is the shortest forwarding path to the source. If the unicast routing metrics is a hop, the forwarding path of source-based tree is the minimum hop; if the unicast routing metrics is delay, the forwarding path of source-based tree is the minimum delay.

For each multicast source, a corresponding multicast forwarding tree is provided to directly connect the source with receivers. All flows transmitted to the designated group are forwarded along the corresponding forwarding tree.

- **Shared tree**: Shared tree depends on RP. All flows are transmitted from a source to an RP, and the RP transmits the flows to receivers. For each multicast group, only one forwarding tree is established, regardless of the count of sources. Shared tree is unidirectional, so that traffic flows from the RP to receivers only. If multicast data from a source is to be transmitted, the multicast data will be transmitted to an RP, and then to receivers from the RP.
- **Bootstrap router (BSR)**: When a multicast source starts sending multicast data or a receiver starts sending a join message to an RP, the multicast router must know the RP information. BSR is responsible for gathering RP information in the network upon PIM-SM network startup, electing an RP for each group, and distributing RP set (namely group-RP mapping database) across the entire PIM-SM network.
- **Data flow from source to receivers:** Sending Hello message: PIM router regularly sends a Hello message to discover PIM router neighbors. Hello message is a multicast message using an address of 224.0.0.13. PIM router responds to Hello messages, and the hold time of Hello messages determines the active time of the messages.
- **Electing designated router:** If there are multiple multicast routers in a multi-access network, only one multicast router will be elected as the designated router to send join/prune messages to an RP for multicast receivers in local network.
- **RP discovery:** PIM-SM generates bootstrap message via bootstrap router and distributes RP message to all multicast routers. Multicast routers receive and store bootstrap messages. When DR receives an IGMP message or multicast data from a direct-connected host, DR will calculate out the RP of the multicast group, and send a join/prune message or encapsulated register message to the RP. Static assigning RP is supported for small network environment.
- **Joining shared tree:** To join a multicast group, the host will send an IGMP message to the upstream router, and the multicast router will send a join message to the upstream PIM neighbor in the RP direction. The multicast router will check whether there is a local multicast group upon receiving the join request from the downstream devices. If there is a local multicast group, it means the join message is sent to the shared tree, and the interface receiving the message becomes an outgoing interface. If there is no local multicast group, entries will be created, the interface receiving the message is added into outgoing, and the join message will be sent to the upstream PIM neighbor in the RP direction.
- **Multicast source registration:** The router directly connected to multicast source S, upon receiving a message from the multicast, will encapsulate the message into a register message and send it to the corresponding RP in unicast mode. When the RP receives the register message from multicast source S, it will de-encapsulate the register message and forward multicast information along RPT tree to receivers, and also send a join message to multicast source hop-by-hop (S, G) so as to enable all routers between the RP and multicast source to generate table entries (S, G). The routers passed through form branches of SPT tree. SPT source tree takes multicast source S as the root, and the RP as destination. The multicast information from multicast source S reaches the RP along the established SPT tree, and the RP forwards the information along RPT shared tree.
- **Sending register-stop message:** If an RP receives a register message from the multicast source and an unencapsulated multicast message thereafter, the RP will send a register-stop message to DR near the multicast source, and DR will stop sending register message to the RP upon receiving the register-stop message.

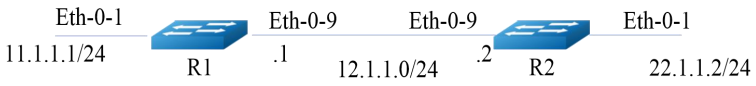
- **Pruning port:** The multicast router on the receiver side sends a prune message to the upstream PIM neighbor in the RP direction. The uplink multicast router, upon receiving the prune message, will delete the interface receiving the prune message as forwarding port. If no other receivers exist on the router, sending prune message to the upstream PIM neighbor in the RP direction will continue.
- **Forwarding multicast data:** PIM-SM router sends multicast data to those explicitly intending to join the multicast group. Multicast router will conduct RPF check, and only the qualified multicast data packets can be sent out via the outgoing port.

5.3.4 Configure General PIM Sparse-mode

I. Configuration

PIM-SM is a soft-state protocol. The essential requirement is to enable PIM-SM protocol on the needed interfaces and correctly configure RP information in static or dynamic manner. The IGMP report/exit and PIM join/prune messages of all multicast groups remain dynamic. We only support all multicast groups of one RP at the moment (224.0.0.0 / 4).

This section provides two related scenes of PIM-SM configuration. The network topology used for the example is as follows:



Configure Static RP

In the example above, R1 is an RP, and all routers are configured with a static RP;

- Every router is configured with a static RP address *11.1.1.1.*
- PIM-SM feature must be enabled on all interfaces.

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 11.1.1.1/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode

Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.1/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	Configure static unicast route
Switch(config)# ip pim rp-address 11.1.1.1	Configure static RP address

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 22.1.1.2/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.2/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	Configure static unicast route
Switch(config)# ip pim rp-address 11.1.1.1	Configure static RP address

II. Check Configuration

All routers are configured with the same RP address 11.1.1.1, and the following command is used to validate the RP configuration, interface details and multicast routing table.

Detailed RP Description

The result of running the “show PIM-SM RP mapping” command on R1 indicates that 11.1.1.1 is the RP configured to all multicast groups 224.0.0.0/4 in static manner. All other routers have a similar output:

R1# show ip pim sparse-mode rp mapping

```
PIM group-to-RP mappings
Group(s): 224.0.0.0/4, Static
  RP: 11.1.1.1
      Uptime: 00:08:21
```

Interface Details

Show multicast information of R1 interface.

R1# show ip pim sparse-mode interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR	HoldTime
11.1.1.1	eth-0-1	2	v2/S	0	1	11.1.1.1	105
12.1.1.1	eth-0-9	0	v2/S	1	1	12.1.1.2	105

IP Multicast Routing Table

Show PIM-SM multicast routing table.

R1# show ip pim sparse-mode mroute detail

```
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
(*, 224.1.1.1) Uptime: 12:01:32 AM
  RP: 11.1.1.1, RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT: off
   Macro state: Join Desired,
  Downstream:
   eth-0-9:
    State: JOINED, ET Expiry: 179 secs, PPT: off
    Assert State: NO INFO, AT: off
     Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
    Macro state: Could Assert, Assert Track
  Join Olist:
   eth-0-9
```

R2# show ip pim sparse-mode mroute detail

```
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
```

```
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
(*, 224.1.1.1) Uptime: 12:00:43 AM
 RP: 11.1.1.1, RPF nbr: 12.1.1.1, RPF idx: eth-0-9
 Upstream:
  State: JOINED, SPT Switch: Enabled, JT Expiry: 18 secs
  Macro state: Join Desired,
 Downstream:
  eth-0-1:
   State: NO INFO, ET: off, PPT: off
   Assert State: NO INFO, AT: off
    Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
   Macro state: Could Assert, Assert Track
 Local Olist:
  eth-0-1
```

5.3.5 Configure Dynamic RP

In a small and simple network, the amount of information is small, and only one RP is needed in the whole network for forwarding information, where the RP position can be specified on routers in SM domain in static manner. In many conditions, however, PIM-SM network is of a large size, and a huge amount of information will be forwarded via RP. To relieve the RP load and optimize the topological structure of the shared tree, different multicast groups should have separate RPs. In this case, the bootstrap mechanism is needed for electing an RP in dynamic manner.

I. Configuration

The below shows detailed configuration of dynamic RP:

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 11.1.1.1/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.1/24	Configure IP address

Switch(config-if)# ip pim sparse-mode	Enter configuration mode
Switch(config-if)# exit	Enter interface mode
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	Configure static unicast route
Switch(config)# ip pim rp-candidate eth-0-1	Configure candidate RP interface

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 22.1.1.2/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.2/24	Configure IP address
Switch(config-if)# ip pim sparse-mode	Enable PIM-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	Configure static unicast route
Switch(config)# ip pim rp-candidate eth-0-9	Configure candidate RP interface
Switch(config)# ip pim bsr-candidate eth-0-9	Configure candidate BSR interface

Select the router of top priority as RP. If two or more routers share the same priority, the Hash Function in BSR mechanism can be used to select RP to ensure that all routers in PIM domain match the same RPs of a group. Use the "**ip pim rp-candidate IFNAME PRIORITY**" command to change the default priority of candidate RP.

II.Check Configuration

PIM-SM's Group-RP Mapping Relation

Use the "**show ip pim sparse-mode rp mapping**" command to show details of Group-RP mapping, and the output is candidate RP information. The group of 224.0.0.0/4 is provided with

two candidate RPs. The default priority of candidate RP 11.1.1.1 is 192, and the priority of candidate RP 12.1.1.2 is configured as 2. Being of a higher priority, candidate RP 12.1.1.2 is selected as the RP of multicast group 224.0.0.0/24.

R2# show ip pim sparse-mode rp mapping

```
PIM group-to-RP mappings
This system is the bootstrap router (v2)
Group(s): 224.0.0.0/4
  RP: 12.1.1.2
    Info source: 12.1.1.2, via bootstrap, priority 2
         Uptime: 01:55:20, expires: 12:02:17 AM
  RP: 11.1.1.1
    Info source: 11.1.1.1, via bootstrap, priority 192
         Uptime: 1:55:23 AM, expires: 12:02:13 AM
```

Detailed RP Display

To display the information of group-specific RP routers, please use the following command. The output indicates that 12.1.1.2 is selected as the RP of 224.1.1.1 multicast group.

R2# show ip pim sparse-mode rp-hash 224.1.1.1

```
  RP: 12.1.1.2
  Info source: 12.1.1.2, via bootstrap
```

RP information will reach all PIM routers in the domain, and the state machines will keep all results of routing join/prune from group members. For displaying detailed interface information and multicast routing table information, please refer to the part of Static RP Configuration above.

5.3.6 Configure Bootstrap Router

Each multicast group needs an RP to serve it, and the RP is taken as the root of the distribution tree based on multicast group. To ensure multicast data from the sender can reach receivers, the multicast routers in one multicast domain need to use the same multicast group-RP mapping. To select an RP for a specific multicast group, multicast routers need to maintain a series of multicast-RP mapping relations, which is called RP set. The mechanism of bootstrap router is to enable multicast routers in the same multicast domain to learn the RP set.

BSR is the core of management in PIM-SM network, mainly responsible for:

- Gathering advertisement messages from Candidate-RP (C-RP) in the network.
- Selecting partial C-RP information for each multicast group and forming an RP-Set (namely multicast group-RP mapping database).
- Notifying all routers (including DR) across the whole PIM-SM network of the RP position.

One PIM domain needs one or more candidate BSRs, and a bootstrap router BSR will be automatically elected from the candidate BSRs to be responsible for gathering and distributing RP information. The below briefs automatic election from candidate BSRs:

- An interface with PIM-SM enabled must be assigned while configuring a router as candidate BSR.

- All candidate BSRs initially regard themselves as a BSR of the PIM-SM and sends bootstrap messages with IP address of the interface as BSR address.
- Candidate BSRs will compare the BSR address of the newly received bootstrap message with their own BSR address when receiving a bootstrap message from other routers for priority and IP address. With the same priority, the larger IP address is regarded better. If the former is better, Candidate BSRs will replace their own BSR address with the new BSR address, and stop regarding themselves as a BSR. Otherwise, they will retain their own BSR address, and continue to regard themselves as a BSR.
- The alternative RP reports its own RP information to the bootstrap router, and the bootstrap router distributes the aggregated RP set to all routers across the multicast domain via bootstrap message.

I. Topology

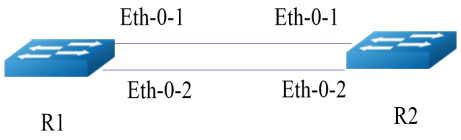


Figure 5-1 BSR Topology

II. Configuration

Router 1

Switch# configure terminal	Enter configuration mode
Switch(config)# ip pim bsr-candidate eth-0-1	Assign candidate BSR interface, with priority of 64 by default

Router 2

Switch# configure terminal	Enter configuration mode
Switch(config)# ip pim bsr-candidate eth-0-1 10 25	Configure BSR candidate interface with HASH mask length of 10 and priority of 25
Switch(config)# ip pim rp-candidate eth-0-1 priority 0	Configure RP candidate interface with priority of 0

Use command "**ip pim unicast-bsm**" to configure the interface to send and receive BSM messages in unicast mode.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode

Switch(config-if)# ip pim dr-priority 10	Configure the priority of interface DR
Switch(config-if)# ip pim unicast-bsm	Configure the interface to send and receive BSM messages in unicast mode

Ⅲ.Check Configuration

Check Candidate BSR Router

Switch# show ip pim sparse-mode bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 20.0.1.21
Uptime: 00:37:12, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:04
Role: Candidate BSR
State: Elected BSR

Check Candidate BSR Router

Switch# show ip pim sparse-mode bsr-router

PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime: 12:02:39 AM, BSR Priority: 64, Hash mask length: 10
Expires: 12:00:03 AM
Role: Candidate BSR
State: Pending BSR
Switch# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime: 12:40:20 AM, BSR Priority: 64, Hash mask length: 10
Expires: 12:02:07 AM
Role: Candidate BSR
State: Candidate BSR

Check RP on E-BSR

Switch# sh ip pim sparse-mode rp mapping

PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
RP: 20.0.1.11
Info source: 20.0.1.11, via bootstrap, priority 0
Uptime: 12:00:30 AM, expires: 12:02:04 AM

Check RP on C-BSR

Switch# show ip pim sparse-mode rp mapping

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 20.0.1.11
Info source: 20.0.1.21, via bootstrap, priority 0
Uptime: 12:00:12 AM, expires: 12:02:18 AM

5.3.7 Configure PIM-SSM

PIM-SSM is realized via portion of PIM-SM technology and IGMPv3. Its process of establishing multicast forwarding tree is similar to that of PIM-SM of establishing SPT tree, that's the receiver DR directly sends a Join message to the multicast data source and sends the multicast data flow to the receiver

after learning about the exact position of the multicast data source.

By default, the range of SSM multicast group address is 232.0.0.0~232.255.255.255. If the multicast group of the user comes within the SSM group address range, processing is conducted via PIM-SSM; if the multicast group of the user falls outside the SSM group address range, processing is conducted via PIM-SM.

PIM-SSM is featured that network users can know the exact position of multicast source in advance. By this, users can explicitly specify the sources of information for receiving before joining a multicast group. The group member end DR will directly send a Join message to the direction of multicast source after knowing users' needs. The Join message is uplinked hop by hop to establish an SPT between the source and group members.

PIM-SSM only uses portion of PIM-SM technology: with no need for RP maintenance, RPT establishment and multicast source registration, with the capability of directly establishing an SPT between the source and group members.

PIM-SSM and PIM-SM can work together on multicast routers. PIM-SSM is disabled by default.

Switch# configure terminal	Enter configuration mode
Switch(config)# ip pim ssm default	Enable PIM-SSM
Switch(config)# ip pim ssm range ipacl	Set PIM-SSM group range according to the assigned acl

5.4 PIM-DM Configuration

5.4.1 Introduction

Protocol independent multicast dense mode (PIM-DM) is a multicast routing protocol for connecting densely distributed multicast devices for collaboration. It helps sparse network nodes save bandwidth and reduce bandwidth usage by transmitting a single flow to multiple receivers.

PIM-DM assumes that when a multicast source starts sending multicast stream, all downstream systems expect to receive the multicast stream. In the beginning, the multicast stream floods

across the entire network. In the case of flooding, PIM-DM uses RPF to prevent loops of multicast stream. If there is no receiving member of the multicast group in some network zones, PIM-DM will delete the forwarding branch by means of pruning.

Pruning state is subject to a life cycle. Upon the life cycle ending, multicast data will start forwarding again. The multicast group corresponding to each (S,G) has its own pruning state. If a new receiver appears in a pruned zone of a multicast group, the router will change the pruning state to forwarding path by sending a “graft” message to the multicast source.

5.4.2 References

PIM-DM module is based on the following IETF standard:

RFC 3973

5.4.3 Configure General PIM Dense-mode

I. Topology

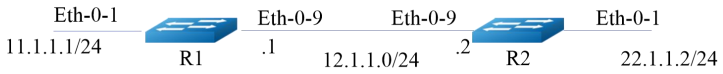


Figure 5-2 Configure PIM Dense-mode

II. Configuration

PIM-DM is a soft-state protocol. The essential requirement is to enable PIM-DM protocol on the needed interfaces. The state of all multicast groups is maintained in dynamic manner via IGMP report/exit and PIM messages.

This section provides two related scenes of PIM-DM configuration. The network topology used for the example is as above;

Multicast stream enters via R1 eth-0-1, and receivers connect to R2 eth-0-2.

A configuration example is as below:

Configuring R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode of eth-0-1
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 11.1.1.1/24	Configure interface IP address
Switch(config-if)# ip pim dense-mode	Enable interface pim dm feature
Switch(config-if)# exit	Exit interface mode

Switch(config)# interface eth-0-9	Enter interface mode of eth-0-9
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.1/24	Configure interface IP address
Switch(config-if)# ip pim dense-mode	Enable interface pim dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	Configure a static route

Configuring R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode of eth-0-1
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 22.1.1.2/24	Configure interface IP address
Switch(config-if)# ip pim dense-mode	Enable interface pim dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode of eth-0-9
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 12.1.1.2/24	Configure interface IP address
Switch(config-if)# ip pim dense-mode	Enable interface pim dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	Configure a static route

III. Check Configuration

Use the following command to check interface configuration and routing table information.

Interface Details

Use the “show ip pim dense-mode interface” command to display interface details on R1.

R1# show ip pim dense-mode interface

```
Address         Interface VIFIndex Ver/   Nbr
                          Mode   Count
11.1.1.1        eth-0-1   0       v2/D   0
12.1.1.1        eth-0-9   1       v2/D   1
```

Neighbor Details

Use the “show ip pim dense-mode neighbor” command to display neighbor details on R1

R1# show ip pim dense -mode neighbor

```
Neighbor-Address Interface          Uptime/Expires    Ver
12.1.1.2         eth-0-9            00:01:00/00:01:44 v2
```

Multicast Routing Table Information

Use the “show ip pim dense-mode mroute detail” command to display the details of PIM-DM multicast routing table

R1# show ip pim dense-mode mroute

```
PIM-DM Multicast Routing Table
(11.1.1.2, 225.1.1.1)
  Source directly connected on eth-0-1
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-1
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-9, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

R2# show ip pim dense-mode mroute

```
PIM-DM Multicast Routing Table
(11.1.1.2, 225.1.1.1)
  RPF Neighbor: none
  Upstream IF: eth-0-9
    Upstream State: AckPending
    Assert State: NoInfo
  Downstream IF List:
    eth-0-1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

5.5 Configure IGMP Snooping

5.5.1 Introduction

IGM Snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism running on layer 2 Ethernet switches for managing and controlling multicast groups.

Layer 2 switches control flooding of multicast stream via IGMP Snooping. If a layer 2 Ethernet switch receives an IGMP message transmitted between a host and routers, IGMP Snooping will analyze the information in the IGMP message, establishing a mapping relationship between the interface and MAC multicast address, and forward multicast data according to this mapping relationship. Multicast routers regularly send general group query to maintain multicast group member relationship. All receivers will respond to the query by sending an IGMP report message, and switches establish forwarding table entries by snooping the IGMP report message.

An Layer 2 multicast group can be established in dynamic manner via IGMP message or configured in static manner. Statically configured multicast groups will override dynamic multicast groups.

5.5.2 Configure Enabling IGMP Snooping

IGMP Snooping can be enabled globally or individually in each VLAN. If IGMP Snooping is disabled in global mode, IGMP Snooping will be inactive even if you enable IGMP Snooping individually in all VLANs. If IGMP Snooping is enabled in global mode, you can disable IGMP Snooping in one VLAN. Besides, global configuration can override configurations of all VLANs. By default, IGMP Snooping is enabled in global mode and individually in each VLAN.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping	Enable IGMP Snooping in global mode
Switch(config)#ip igmp snooping vlan 1	Enable IGMP Snooping in individual VLAN
Switch # show ip igmp snooping vlan 1	Check configuration

II. Command validation

Switch # show ip igmp snooping vlan 1

```
Global Igmp Snooping Configuration
----------------------------------------------------
Igmp Snooping                          :Enabled
Igmp Snooping Fast-Leave               :Disabled
Igmp Snooping Version                  :2
Igmp Snooping Robustness Variable      :2
Igmp Snooping Max-Member-Number        :2048
Igmp Snooping Unknown Multicast Behavior  :Flood
```

```
Igmp Snooping Report-Suppression          :Enabled
Vlan 1
----------
Igmp Snooping                             :Enabled
Igmp Snooping Fast-Leave                  :Disabled
Igmp Snooping Report-Suppression          :Enabled
Igmp Snooping Version                     :2
Igmp Snooping Robustness Variable         :2
Igmp Snooping Max-Member-Number           :2048
Igmp Snooping Unknown Multicast Behavior  :Flood
Igmp Snooping Group Access-list           :N/A
Igmp Snooping Mrouter Port                :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

5.5.3 Configure IGMP Snooping Fast Leave

Under normal circumstances, IGMP Snooping will not directly delete an interface from a multicast group after receiving an IGMP exit message, but send an IGMP group-specific query message and delete the interface from the multicast group if no response is received after a period of time. If the quick delete function is enabled, IGMP Snooping will directly delete an interface from a multicast group upon receiving an IGMP message. If there is only one user under the interface, quick delete helps saving bandwidth.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)#ip igmp snooping fast-leave	Enable fast leave in global mode
Switch(config)#ip igmp snooping vlan 1 fast-leave	Enable fast leave in VLAN mode
Switch # show ip igmp snooping vlan 1	Check configuration

II. Command validation

Switch # show ip igmp snooping vlan 1

```
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                             :Enabled
Igmp Snooping Fast-Leave                  :Enabled
Igmp Snooping Version                     :2
Igmp Snooping Robustness Variable         :2
Igmp Snooping Max-Member-Number           :2048
Igmp Snooping Unknown Multicast Behavior  :Flood
Igmp Snooping Report-Suppression          :Enabled
Vlan 1
----------
Igmp Snooping                             :Enabled
Igmp Snooping Fast-Leave                  :Enabled
Igmp Snooping Report-Suppression          :Enabled
Igmp Snooping Version                     :2
Igmp Snooping Robustness Variable         :2
```

```
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Group Access-list              :N/A
Igmp Snooping Mrouter Port                   :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

5.5.4 Configure IGMP Snooping Query Parameters

Layer 3 switches periodically send general IGMP query messages in the connected network segment, and learn about which multicast groups have members in the segment by resolving the returned IGMP host report messages. Multicast routers periodically send query messages and refresh the corresponding group member relationship information in the network segment when receiving an IGMP host report message from a group member.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping query-interval 100	Set query interval as 100 seconds
Switch(config)# ip igmp snooping query-max-response-time 5	Set maximum response time as 5 seconds
Switch(config)#ip igmp snooping last-member-query-interval 2000	Set last member query interval
Switch(config)#ip igmp snooping vlan 1 querier address 10.10.10.1	Configure IGMP Snooping querier address in VLAN1
Switch(config)#ip igmp snooping vlan 1 querier	Enable IGMP Snooping querier on VLAN1
Switch(config)#ip igmp snooping vlan 1 query-interval 200	Set query interval of VLAN1 as 200 seconds
Switch(config)#ip igmp snooping vlan 1 query-max-response-time 5	Set maximum response time of VLAN1 as 5 seconds
Switch(config)#ip igmp snooping vlan 1 querier-timeout 100	Set queirer timeout of VLAN1 as 100 seconds
Switch(config)#ip igmp snooping vlan 1 last-member-query-interval 2000	Set group-specific query interval of VLAN1 as 2000 seconds
Switch(config)# ip igmp snooping vlan 1 discard-unknown	Discard unknown multicast message on VLAN1
Switch(config)# ip igmp snooping discard-unknown	Discard unknown multicast message in global mode

II. Command validation

Switch # show ip igmp snooping querier

```
Global Igmp Snooping Querier Configuration
-------------------------------------------------
Version                     :2
Last-Member-Query-Interval (msec)    :2000
Last-Member-Query-Count              :2
Max-Query-Response-Time (sec)        :5
Query-Interval (sec)                 :100
Global Source-Address                :0.0.0.0
TCN Query Count                      :2
TCN Query Interval (sec)             :10
TCN Query Max Respose Time (sec)  :5
Vlan 1:   IGMP snooping querier status
-------------------------------------------
Elected querier is : 0.0.0.0
-------------------------------------------
Admin state                          :Enabled
Admin version                        :2
Operational state                    :Non-Querier
Querier operational address          :10.10.10.1
Querier configure address            :10.10.10.1
Last-Member-Query-Interval (msec) :2000
Last-Member-Query-Count              :2
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)                 :200
Querier-Timeout (sec)                :100
```

5.5.5 Configure IGMP Snooping Multicast Routed Ports

Multicast routed ports refer to switch ports connecting to multicast routers, which can be dynamically learned or statically configured. If a port of a VLAN receives a general IGMP query message or PIMv2 Hello message, the port becomes the multicast routed port of the VLAN. All IGMP query messages received via multicast routed port will be broadcast in the VLAN. All IGMP report/exit messages received on the VLAN also will be forwarded from the multicast routed port (with message suppression disabled), and all multicast flows received from the VLAN will be forwarded from the multicast routed port.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping report-suppression	Enable IGMP Snooping report suppression
Switch(config)# ip igmp snooping vlan 1 mrouter interface eth-0-1	Configure static multicast router interface
Switch(config)# ip igmp snooping vlan 1 report-suppression	Enable report suppression on VLAN1
Switch(config)# ip igmp snooping vlan 1 mrouter-aging-interval 200	Configure dynamic multicast router aging interval

II. Command validation

Switch# show ip igmp snooping vlan 1

```
Global Igmp Snooping Configuration
-----------------------------------------------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
Vlan 1
----------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Report-Suppression             :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Group Access-list              :N/A
Igmp Snooping Mrouter Port                   :eth-0-1
Igmp Snooping Mrouter Port Aging Interval(sec) :200
```

5.5.6 Configure IGMP Snooping Query TCN

Multicast group learning and updating after STP convergence topology can be adapted to by configuring TCN interval and query count.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping querier tcn query-count 5	Set TCN query count
Switch(config)# ip igmp snooping querier tcn query-interval 20	Set TCN query interval as 20 seconds

II. Command validation

Switch # show ip igmp snooping querier

```
Global Igmp Snooping Querier Configuration
-----------------------------------------------
Version                          :2
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)    :10
Query-Interval (sec)             :125
Global Source-Address            :0.0.0.0
TCN Query Count                  :5
```

```
TCN Query Interval (sec)        :20
Vlan 1:   IGMP snooping querier status
-----------------------------------------
Elected querier is : 0.0.0.0
-----------------------------------------
Admin state                     :Disabled
Admin version                   :2
Operational state               :Non-Querier
Querier operational address     :0.0.0.0
Querier configure address       :N/A
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)   :10
Query-Interval (sec)            :125
Querier-Timeout (sec)           :255
```

5.5.7 Configure IGMP Snooping Report Suppression

Switches use IGMP report suppression to prevent repeatedly sending same IGMP messages to multicast routers. If IGMP router suppression is enabled (by default), a switch sends the first IGMP report message to a multicast router, and other same IGMP report messages will not be sent to the multicast router. In this way, duplicate IGMP report messages will not be sent to the multicast router.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping report-suppression	Enable report suppression in global mode
Switch(config)# ip igmp snooping vlan 1 report-suppression	Enable report suppression in VLAN1 mode

II. Command validation

Switch # show ip igmp snooping

```
Global Igmp Snooping Configuration
-------------------------------------------------
Igmp Snooping                          :Enabled
Igmp Snooping Fast-Leave               :Disabled
Igmp Snooping Version                  :2
Igmp Snooping Robustness Variable      :2
Igmp Snooping Max-Member-Number        :2048
Igmp Snooping Unknown Multicast Behavior  :Flood
Igmp Snooping Report-Suppression       :Enabled
Vlan 1
----------
Igmp Snooping                          :Enabled
Igmp Snooping Fast-Leave               :Disabled
Igmp Snooping Report-Suppression       :Enabled
Igmp Snooping Version                  :2
```

```
Igmp Snooping Robustness Variable              :2
Igmp Snooping Max-Member-Number                :2048
Igmp Snooping Unknown Multicast Behavior       :Flood
Igmp Snooping Group Access-list                :N/A
Igmp Snooping Mrouter Port                     :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
```

5.5.8 Configure Static Multicast Group

Switches will establish IGMP Snooping group records when receiving IGMP messages via layer 2 ports. The current system also supports statically configuring IGMP Snooping group records, for which group address, layer 2 port and the VLAN of the layer 2 port must be assigned.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ip igmp snooping vlan 1 static-group 229.1.1.1 interface eth-0-2	Configure static multicast 229.1.1.1, with vlan1 eth-0-2 as a member interface

II. Command validation

Switch# show ip igmp snooping groups

```
VLAN  Interface    Group-Address     Uptime     Expires-time
1     eth-0-2      229.1.1.1         00:01:08   stopped
```

5.5.9 Restriction and Configuration Guide

Multicast IP is used in VRRP, RIP and OSPF protocols. Be sure not to use such multicast IP in networks with IGMP Snooping enabled, because the mapped MAC of such multicast IP is consistent with that of multicast IP used by protocol module.

VRRP uses 224.0.0.18, so the mapped multicast IP of multicast MAC 0100.5E00.0012 should be avoided in IGMP Snooping and VRRP networks.

RIP uses 224.0.0.9, so the mapped multicast IP of multicast MAC 0100.5E00.0009 should be avoided in IGMP Snooping and RIP networks.

OSPF uses 224.0.0.5, so the mapped multicast IP of multicast MAC 0100.5E00.0005 should be avoided in IGMP Snooping and OSPF networks.

5.6 Configure MVR

5.6.1 Introduction

In conventional multicast-on-demand mode, some access switches are linked under an aggregation multicast router, and the access switches are connected with users distributed in different VLANs. When users from those VLANs request a program of a same group, the

aggregation multicast router needs to make a copy of data for users in each VLAN, and the multicast traffic from each VLAN will occupy the bandwidth of the access switches. This increases the load of the aggregation router and wastes the bandwidth of the access devices.

Multicast VLAN registration (MVR) feature can solve this problem well. Enable multicast VLAN on the access switch near the user side. The aggregation router needs to send multicast data in source VLAN to the access switch rather than make a copy in every user VLAN, and the access switch will make copies upon user request after receiving the multicast data and send a copy to users in every VLAN. This saves bandwidth usage and lowers the load of layer 3 devices.

MVR running relies on IGMP Snooping, and will be valid in groups with MVR globally configured. If the multicast group in the IGMP message received via the downstream port of MVR is not with MVR globally configured, the message will be ignored. Receiver information is maintained via IGMP report/exit message received via the downstream port of MVR. MVR upstream port will determine the VLANs for forwarding multicast data based on the multicast group information on the downstream port after receiving multicast data.

5.6.2 Terms

MVR: Multicast VLAN registration

Source vlan: Source VLAN of multicast VLAN

Source port: Upstream port in MVR network for connecting with multicast router port

Receiver port: Downstream port in MVR network for connecting with receiver port

5.6.3 Topology

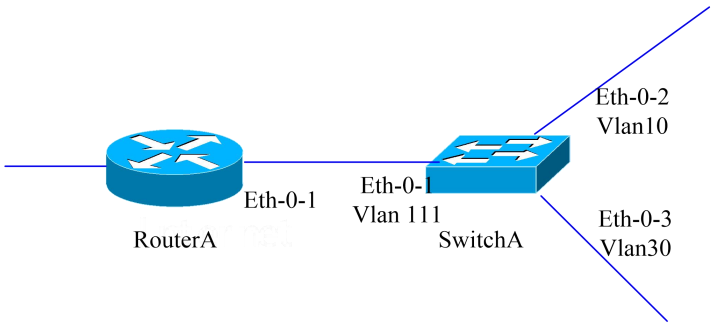


Figure 5-3 Multicast VLAN Topology

5.6.4 Configuration

Destination

Enable IGMP&PIM-SM on Router A eth-0-1.

Configure Switch A: eth-0-1 to belongs to vlan111, eth-0-2 to vlan10, and eth-0-3 to vlan30.

Enable MVR on Switch A, make a copy of multicast stream from Router A to Switch A, and duplicate the multicast stream on Switch A and send it from eth-0-2 and eth-0-3.

Router A

Enable IGMP&PIM-SM on configuration interface.

RouterA# configure terminal	Enter configuration mode
RouterA(config)# interface eth-0-1	Enter interface mode
RouterA(config-if)# no switchport	Set the interface as layer3 interface
RouterA(config-if)# no shutdown	Enable the interface
RouterA(config-if)# ip address 12.12.12.12/24	Configure IP address
RouterA(config-if)# ip pim sparse-mode	Enable PIM-SM protocol
RouterA(config-if)# end	Go back to global mode

Switch A

Configure eth-0-1 to belong to vlan111, eth-0-2 to vlan10, and eth-0-3 to vlan30.

SwitchA# configure terminal	Enter configuration mode
SwitchA(config)# vlan database	Enter VLAN mode
SwitchA(config-vlan)# vlan 111,10,30	Create vlan 111, 10, 30
SwitchA(config-vlan)# quit	Exit VLAN mode
SwitchA(config)# interface vlan 111	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface vlan 10	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface vlan 30	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface eth-0-1	Enter interface mode
SwitchA(config-if)# switchport access vlan111	Set the interface to belong to VLAN111
SwitchA(config)# interface eth-0-2	Enter interface mode
SwitchA(config-if)# switchport access vlan10	Set the interface to belong to VLAN10
SwitchA(config)# interface eth-0-3	Enter interface mode
SwitchA(config-if)# switchport access vlan30	Set the interface to belong to VLAN30
SwitchA(config-if)# end	Exit interface mode

Enable MVR on Switch A, so that only one copy of multicast stream will be made from Router A to Switch A, and the multicast stream will be sent from eth-0-2 and eth-0-3 on Switch A.

SwitchA# configure terminal	Enter configuration mode
SwitchA(config)# no ip multicast-routing	Shut down IP multicast routing
SwitchA(config)# mvr	Enable MVR
SwitchA(config)# mvr vlan 111	Create MVR VLAN
SwitchA(config)# mvr group 238.255.0.1 64	Create multicast group
SwitchA(config)# mvr source-address 12.12.12.1	Configure MVR source address
SwitchA(config)# interface eth-0-1	Enter interface mode
SwitchA(config-if)# mvr type source	Configure the interface as MVR source interface
SwitchA(config)# interface eth-0-2	Enter interface mode
SwitchA(config-if)# mvr type receiver vlan 10	Configure the interface as MVR receiver interface
SwitchA(config)# interface eth-0-3	Enter interface mode
SwitchA(config-if)# mvr type receiver vlan 30	Configure the interface as MVR receiver interface
SwitchA(config-if)# end	Exit interface mode

5.6.5 Command Validation

Router A

RouterA # show ip igmp groups

IGMP Connected Group Membership

Group Address	Interface	Uptime	Expires	Last Reporter
238.255.0.1	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.2	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.3	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.4	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.5	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.6	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.7	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.8	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.9	eth-0-1	00:01:16	00:03:49	12.12.12.1
238.255.0.10	eth-0-1	00:01:16	00:03:49	12.12.12.1

……

238.255.0.64 eth-0-1 00:01:16 00:03:49 12.12.12.1

Switch A

SwitchA# show mvr

MVR Running: TRUE
MVR Multicast VLAN: 111
MVR Source-address: 12.12.12.1
MVR Max Multicast Groups: 1024
MVR Hw Rt Limit: 508
MVR Current Multicast Groups: 255

SwitchA# show mvr groups

VLAN	Interface	Group-Address	Uptime	Expires-time
10	eth-0-2	238.255.0.1	00:03:23	00:02:03
10	eth-0-2	238.255.0.2	00:02:16	00:02:03
10	eth-0-2	238.255.0.3	00:02:16	00:02:03
10	eth-0-2	238.255.0.4	00:02:16	00:02:03
10	eth-0-2	238.255.0.5	00:02:16	00:02:03
10	eth-0-2	238.255.0.6	00:02:16	12:02:04 AM
10	eth-0-2	238.255.0.7	00:02:16	12:02:04 AM
10	eth-0-2	238.255.0.8	00:02:16	12:02:04 AM
10	eth-0-2	238.255.0.9	00:02:16	12:02:04 AM
10	eth-0-2	238.255.0.10	00:02:16	00:02:04
……				
10	eth-0-2	238.255.0.64	00:01:50	00:02:2

6 Security Configuration Guide

6.1 Port Security Configuration

6.1.1 Introduction

The port security feature is for limiting the number of reliable MAC addresses of a specific interface. The interface will only forward data packets from safe addresses matching the source MAC address. MAC address can be created manually or learned automatically. If the number of MAC addresses reach the safe MAC address limit, new MAC addresses cannot be learned on the interface. If the interface receives a new data packet, and the data packet source MAC address is different from any safe address, it will be regarded to violate security.

Port security binds MAC addresses with the interface, and messages with an MAC address not included in these addresses will not be forwarded after entering via the interface. If a safe MAC address has been learned on the interface, but the MAC address attempts to learn from or configure to another interface, this also is regarded to violate security.

The supported safe MAC address types include:

- Safe static MAC addresses: refer to manually configured MAC addresses.
- Safe dynamic MAC addresses: relate to dynamic learning.

In the case of security violation, the data packets to be forwarded will be discarded.

6.1.2 Configuration

Conduct the following steps to configure port security.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport	Set the interface as layer2 interface
Switch(config-if)# switchport port-security	Enable port security
Switch(config-if)# switchport port-security maximum 3	Set maximum security entries
Switch(config-if)# switchport port-security mac-address 0000.1111.2222 vlan 1	Bind MAC address with the interface

Switch(config-if)# switchport port-security mac-address 0000.aaaa.bbbb vlan 1	Bind MAC address with the interface
Switch(config-if)# switchport port-security violation restrict	Set port restrict mode
Switch(config-if)# end	Exit interface mode
Switch# show port-security	Check configuration

6.1.3 Command Validation

Switch# show port-security

```
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolationMode
             (Count)        (Count)
---------------------------------------------------------------
  eth-0-1          3             2       restrict
Switch# show port-security address-table
        Secure MAC address table
------------------------------------------------------------
Vlan    Mac Address       Type                Ports
----    -----------       -------             -------
1       0000.1111.2222    SecureConfigured    eth-0-1
1       0000.aaaa.bbbb    SecureConfigured    eth-0-1
```

Switch# show port-security interface eth-0-1

```
Port security                       : enabled
Violation mode                      : discard packet and log
Maximum MAC addresses               : 3
Total MAC addresses                 : 2
Static configured MAC addresses     : 2
```

6.2 VLAN Security Configuration

6.2.1 Introduction

VLAN security feature attains the goal of VLAN protection by limiting the number of MAC addresses in VLAN. MAC address can be manually added by users or automatically learned. If the limit of MAC addresses in a VLAN is reached, messages from unknown source MAC will be discarded (assignable behavior).

The system supports two types of MAC addresses:

- Static MAC addresses: refer to manually configured MAC addresses
- Dynamic MAC addresses: relate to dynamically learned MAC addresses

Users can assign one of the following actions if the limit of MAC addresses in a VLAN is reached:

- Discard: Discard messages from unknown source MAC address

- Warn: Discard messages from unknown source MAC address, and give a warning in LOG
- Forward: Forward messages but do not learn the MAC.

The system also supports turning on/off MAC address learning in VLAN.

6.2.2 Configure VLAN MAC Address Limit

The below shows steps of configuring MAC address limit.

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config)# vlan 2	Create VLAN2
Switch(config-vlan)# vlan 2 mac-limit maximum 100	Configure maximum MAC addresses of VLAN2
Switch(config-vlan)# vlan 2 mac-limit action discard	Assign discard action if the limit is reached
Switch(config-vlan)#end	Exit VLAN mode
Switch #show vlan-security	Check configuration

6.2.3 Configure VLAN MAC Address Learning

The below shows steps of disabling MAC address learning of VLAN.

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config)# vlan 2	Create VLAN
Switch(config-vlan)# vlan 2 mac learning disable	Disable MAC address learning
Switch(config-vlan)#end	Exit VLAN mode
Switch #show vlan-security	Check configuration

6.2.4 Command Validation

Switch #show vlan-security

```
Vlan  learning-en  max-mac-count  cur-mac-count  action
-------------------------------------------------------
```

2 Disable 100 0 Discard

6.3 Time-Range Configuration

6.3.1 Introduction

Time range defines a period of time, which can be an absolute time or relatively periodic time. Time range is meaningless itself, and is usually used in time-based protocols or applications (such as acl). In practical application, it can indicate some rules or actions are valid during this period. The time defined via time range depends on the system clock.

6.3.2 Configuration

Configure An Absolute Time Range

Switch# configure terminal	Enter global configuration mode
Switch(config)# time-range test-absolute	Create time-range to enter time range configuration mode
Switch(config-tm-range)# absolute start 1:1:2 jan 1 2012 end 1:1:3 jan 7 2012	Create an absolute time
Switch(config-tm-range)# end	Exit time range configuration mode

Configure A Periodic Time Range

Switch# configure terminal	Enter global configuration mode
Switch(config)# time-range test-periodic	Create time-range to enter time range configuration mode
Switch(config-tm-range)# periodic 1:1 mon to 1:1 wed	Create a periodic time
Switch(config-tm-range)# end	Exit time range configuration mode

6.3.3 Command Validation

DUT1# show time-range

```
time-range test-absolute
  absolute start 01:01:02 Jan 01 2012 end 01:01:03 Jan 07 2012
time-range test-periodic
  periodic 01:01 Mon to 01:01 Wed
```

6.4 Access Control List Configuration

6.4.1 Introduction

Access control list (ACL) is mainly used for realizing flow identification and access control. To filter data packets, network devices need to be configured with a series matching rules for identifying messages to be filtered. After identifying specific messages, it can be decided to permit or inhibit corresponding data packets to pass through as per the pre-established policies. ACL classifies data packets by a series of matching conditions such as source address, destination address or port number of data packets.

6.4.2 Terms

The below briefs the terms and concepts related to ACL:

Access Control Entry (ACE)

Each ACE consists of an action element (permit or deny) and a standard-based filter element such as source address, destination address, protocol, specific protocol parameter, etc.

MAC ACL

MAC ACL can filter messages by MAC-SA or MAC-DA, and an MAC address can configure masks or be configured as a host MAC. MAC ACL also can filter messages by other layer 2 fields, such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type.

IPv4 ACL

IPv4 ACL can filter messages by IP-SA or IP-DA, and an IP address can configure masks or be configured as a host IP address. IPv4 ACL also can filter messages by other layer 3 fields, such as DSCP, L4 Protocol fields or other fields (TCP port, UDP port, etc.).

Time Range

Defines a time period when ACE is valid.

6.4.3 Limit

If an incoming message contains only one VLAN tag, fields inner-cos and inner-vlan-id will be set to 0 by default. Thus, the results of inner-vlan-id and inner-cos configuration vary with the count of vlan tags (one or two) in messages.

6.4.4 Configuration

In the following example, MAC ACL is used on on eth-0-1 to permit messages from a source MAC address of 0000.0000.1111 to pass through, and deny other messages. IPv4 ACL is used on eth-0-2 to permit messages from a source IP address of 1.1.1.1/24 to pass through, and deny other messages.

ACL Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch(config)# mac access-list mac	Create and enter MAC ACL configuration mode
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	Add entries, and permit frames from a source MAC address of 0000.0000.1111
Switch(config-mac-acl)# deny src-mac any dest-mac any	Add entries, and deny any MAC frame
Switch(config-mac-acl)# exit	Exit ACL configuration mode
Switch(config)# ip access-list ipv4	Create and enter IPv4 ACL configuration mode
Switch(config-ip-acl)# permit any 1.1.1.1 0.0.0.255 any	Add entries, and permit frames from a source IP address of 1.1.1.1 0.0.0.255
Switch(config-ip-acl)# deny any any any	Add entries, and deny any frame
Switch(config-ip-acl)# exit	Exit ACL configuration mode

Interface Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map cmap1	Create class-map cmap1, and enter class-map configuration mode
Switch(config-cmap)# match access-group mac	Add MAC ACL into cmap1
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap1	Create policy-map pmap1, and enter policy-map configuration mode
Switch(config-pmap)# class cmap1	Add cmap1 into pmap1, and enter the class map configuration mode in the policy map
Switch(config-pmap-c)# exit	Exit the class map configuration mode in the policy map
Switch(config-pmap)# exit	Exit policy map configuration mode
Switch(config)# interface eth-0-1	Enter the port configuration mode of the interface to apply the ACL
Switch(config-if)# service-policy input pmap1	Apply pmap1 to the interface. Since cmap1 is cited in pmap1, and mac ACL is cited in cmap1, mac ACL is applied to the

	interface.
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# class-map cmap2	Create class-map cmap1, and enter class-map configuration mode
Switch(config-cmap)# match access-group ipv4	Add ACL ipv4 into cmap2
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap2	Create policy-map pmap2, and enter policy-map configuration mode
Switch(config-pmap)# class cmap2	Add cmap2 into pmap2, and enter the class map configuration mode in the policy map
Switch(config-pmap-c)# exit	Exit the class map configuration mode in the policy map
Switch(config-pmap)# exit	Exit policy map configuration mode
Switch(config-if)# interface eth-0-2	Enter the port configuration mode of the interface to apply the ACL
Switch(config-if)# service-policy input pmap2	Apply pmap1 to the interface. Since cmap2 is cited in pmap2, and ACL ipv4 is cited in cmap2, ACL ipv4 is applied to the interface.

6.4.5 Command Validation

By running the command “show running-config”, the display content is as below.

Switch# show running-config

```
mac access-list mac
 10 permit src-mac host 0000.0000.1111 dest-mac any
 20 deny src-mac any dest-mac any
!
ip access-list ipv4
 10 permit any 1.1.1.0 0.0.0.255 any
 20 deny any any any
!
class-map match-any cmap1
 match access-group mac
!
class-map match-any cmap2
 match access-group ipv4
!
policy-map pmap1
 class cmap1
!
```

```
policy-map pmap2
 class cmap2
!
interface eth-0-1
 service-policy input pmap1
!
interface eth-0-2
 service-policy input pmap2
!
```

6.5 Extend ACL Configuration

6.5.1 Introduction

Extend IPV4 ACL contains MAC ACE and IP MAC. MAC ACE matches all non-IPV6 and non-MPLS messages, and IP ACE matches all IPV4 messages.

6.5.2 Terms

The below briefs the terms and concepts related to extend ACL:

Extend IPV4 ACL: contains MAC ACE and IP ACE.

MAC ACE can filter messages by MAC-SA or MAC-DA, and an MAC address can configure masks or be configured as a host MAC; also can filter messages by other layer 2 fields, such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type.

IPv4 ACE can filter messages by IP-SA or IP-DA, and an IP address can configure masks or be configured as a host IP address; also can filter messages by other layer 3 fields, such as DSCP, L4 Protocol fields or other fields (TCP port, UDP port, etc.).

Users can address different needs via various combinations of MAC ACE and IP ACE in different orders.

6.5.3 Configuration

The example below shows how to permit messages with a source MAC of 0.0.1111 and COS of 2 and all TCP messages and deny other messages on interface eth-0-1 via extend IPV4 ACL.

Extend ACL Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip access-list ipxacl extend	Define an extend IPV4 ACL named ipxacl
Switch(config-ex-ip-acl)# permit src-mac host 0000.0000.1111 dest-mac any cos 2	Add an ACE to permit messages with source MAC MAC0.0.1111 and cos 2
Switch(config-ex-ip-acl)# permit tcp any any	Add an ACE to permit TCP messages
Switch(config-ex-ip-acl)# deny src-mac any dest-mac any	Add an ACE to deny any messages

Switch(config-ex-ip-acl)# end	Exit to privilege mode

Interface Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map cmap	Create class-map cmap, and enter class-map configuration mode
Switch(config-cmap)# match access-group ipxacl	Add ipxacl ACL into cmap
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap	Create policy-map pmap1, and enter policy-map configuration mode
Switch(config-pmap)# class cmap	Add cmap1 into pmap1, and enter the class map configuration mode in the policy map
Switch(config-pmap-c)# exit	Exit the class map configuration mode in the policy map
Switch(config-pmap)# exit	Exit policy map configuration mode
Switch(config)# interface eth-0-1	Enter the port configuration mode of the interface to apply the ACL
Switch(config-if)# service-policy input pmap	Apply pmap1 into the interface. Since cmap1 is cited in cmap1, and ACL mac is cited in cmap1, ACL mac1 is applied to the interface.
Switch(config-if)# exit	Exit interface configuration mode

6.5.4 Command Validation

Validate the configuration result with the following command.

Switch# show running-config

```
ip access-list ipxacl extend
 10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
 20 permit tcp any any
 30 deny src-mac any dest-mac any
!
class-map match-any cmap
 match access-group ipxacl
!
policy-map pmap
 class cmap
```

```
!
interface eth-0-1
 service-policy input pmap
!
Switch# show access-list ip
ip access-list ipxacl extend
  10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
  20 permit tcp any any
  30 deny src-mac any dest-mac any
```

6.6 Access Control List v6 Configuration

6.6.1 Introduction

ACLv6 (Access control list) is mainly used for realizing IPv6 flow identification and access control. To filter data packets, network devices need to be configured with a series matching rules for identifying messages to be filtered. After identifying specific messages, it can be decided to permit or inhibit corresponding data packets to pass through as per the pre-established policies. ACL classifies data packets by a series of matching conditions such as source address, destination address or port number of data packets.

6.6.2 Terms

The below briefs the terms and concepts related to ACLv6:

Access Control Entry (ACE)

Each ACE consists of an action element (permit or deny) and a standard-based filter element such as source address, destination address, protocol, specific protocol parameter, etc.

IPv6 ACL

IPv6 ACL can filter messages by IP-SA or IP-DA, and an IP address can configure masks or be configured as a host IP address. IPv6 ACL can filter messages by other layer 3 fields, such as L4 Protocol fields or other fields (TCP port, UDP port, etc.).

Time Range

Defines a time period when ACE is valid.

6.6.3 Limit

If IPv6 is globally enabled, IPv6 messages will not be affected by MAC ACL.

6.6.4 Configuration

In the following example, MAC ACL is used on on eth-0-1 to permit non-IPv6 messages from a source MAC address of 0000.0000.1111 to pass through, and deny other non-IPv6 messages.

IPv6 ACL is used on eth-0-2 to permit messages from a source IP address of 2001::/64 to pass through, and deny other messages.

ACL Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch# ipv6 enable	Globally enable IPv6
Switch(config)# mac access-list mac	Create and enter MAC ACL configuration mode
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	Add entries, and permit frames to a destination MAC address of 0000.0000.1111
Switch(config-mac-acl)# deny src-mac any dest-mac any	Add entries, and deny any MAC frame
Switch(config-mac-acl)# exit	Exit ACL configuration mode
Switch(config)# ipv6 access-list ipv6	Create and enter IPv4 ACL configuration mode
Switch(config-ipv6-acl)# permit any 2001::/64 any	Add entries, and permit frames with a source IPv6 address of 2001::/ 64
Switch(config-ipv6-acl)# deny any any any	Add entries, and deny any frame
Switch(config-ipv6-acl)# exit	Exit ACL configuration mode

Interface Configuration Rules

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map cmap1	Create class-map cmap1, and enter class-map configuration mode
Switch(config-cmap)# match access-group mac	Add MAC ACL into cmap1
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap1	Create policy-map pmap1, and enter policy-map configuration mode
Switch(config-pmap)# class cmap1	Add cmap1 into pmap1, and enter the class map configuration mode in the policy map
Switch(config-pmap-c)# exit	Exit the class map configuration mode in the policy map
Switch(config-pmap)# exit	Exit policy map configuration mode

Switch(config)# interface eth-0-1	Enter the port configuration mode of the interface to apply the ACL
Switch(config-if)# service-policy input pmap1	Apply pmap1 into the interface. Since cmap1 is cited in pmap1, and mac ACL is cited in cmap1, mac ACL is applied to the interface.
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# class-map cmap2	Create class-map cmap1, and enter class-map configuration mode
Switch(config-cmap)# match access-group ipv6	Add ACL ipv6 into cmap2
Switch(config-cmap)# exit	Exit class-map configuration mode
Switch(config)# policy-map pmap2	Create policy-map pmap2, and enter policy-map configuration mode
Switch(config-pmap)# class cmap2	Add cmap2 into pmap2, and enter the class map configuration mode in the policy map
Switch(config-pmap-c)# exit	Exit the class map configuration mode in the policy map
Switch(config-pmap)# exit	Exit policy map configuration mode
Switch(config-if)# interface eth-0-2	Enter the port configuration mode of the interface to apply the ACL
Switch(config-if)# service-policy input pmap2	Apply pmap1 into the interface. Since cmap2 is cited in pmap2, and ACL ipv4 is cited in cmap2, ACL ipv4 is applied to the interface.

6.6.5 Command Validation

By running the command “show running-config”, the display content is as below.

Switch# show running-config

```
mac access-list mac
 10 permit src-mac host 0000.0000.1111 dest-mac any
 20 deny src-mac any dest-mac any
!
ipv6 access-list ipv6
 10 permit any 2001::/64 any
 20 deny any any any
!
class-map match-any cmap1
 match access-group mac
!
```

```
class-map match-any cmap2
 match access-group ipv4
!
policy-map pmap1
 class cmap1
!
policy-map pmap2
 class cmap2
!
interface eth-0-1
 service-policy input pmap1
!
interface eth-0-2
 service-policy input pmap2
!
```

6.7 Dot1x Configuration

6.7.1 Introduction

In real deployment of IEEE 802 network, it is unavoidable that unauthorized devices will physically access the network.

802.1X protocol provides a port-based network access control protocol. “Port-based network access control protocol” refers to exercising authentication and control over accessed user equipment at the level of port of LAN access equipment. User equipment having passed the authentication can access the resources in the LAN; in case of failure in authentication, they cannot access the resources in the LAN.

Systems with 802.1x are of a typical Client/Server architecture, and includes three entities:

- Client device (PC) requests to access LAN and switches services and responds to requests from switches. Workstation must run client software complying with 802.1x, such as xsupplicant of Linux.
- Authentication server - executes authentication of clients. Authentication server verifies client identity and notify whether a switch client has access to an LAN and switches services. Since switches act as agent, authentication is transparent to clients. In this version, the remote authentication dial in user service (RADIUS) server that supports the extensible authentication protocol (EAP) is the only supported authentication server. RADIUS runs in client/server mode to switch safe authentication information between the server and multiple RADIUS clients.
- Switches (edge switch or wireless access point) - control physical access of client-based authentication status network. As the intermediary (agent) between clients and authentication server, switches request identity information from clients, check the information via the authentication server, and return the authentication result to clients. Switches contain RADIUS clients, and are responsible for encapsulating and de-encapsulating EAP frames, and interacting with authentication server. When switches receive EAPOL frames and relay it to authentication server, the Ethernet message header will be removed, and the remaining EAP frames will be re-encapsulated in RADIUS format. EAP frames will not be modified or reviewed during encapsulation, and the authentication server must support the frame format of EAP on the machine. Switches will

delete the frame header of server from the message from an authentication server, and encapsulate the remaining EAP frames in the format of Ethernet message and send it to client. We also can configure dotlx on routed ports.

6.7.2 Topology

Figure 6-1 Basic dotlx Topological Graph

6.7.3 Configuration

The steps of enabling dotlx on common layer 2 ports are as below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# dot1x system-auth-ctrl	Globally enable dotlx authentication control
Switch(config)# interface eth-0-25	Assign an interface to be configured, and enter interface configuration mode
Switch(config)# switchport mode access	Set eth-0-25 as access mode
Switch(config-if)# dot1x port-control auto	Enable dotlx port control on the interface
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface vlan 1	Enter VLAN 1
Switch(config-if)# ip address 192.168.100.1/24	Set VLAN1 IP address
Switch(config)# interface eth-0-26	Enter interface configuration mode.
Switch(config-if)# no switchport	Configure the interface as routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure IP address on this interface
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# exit	Exit interface configuration mode.
Switch(config)# radius-server host 202.38.100.7	Configure IPv4 address of RADIUS server

Switch(config)# radius-server host 2001:1000::1	Configure IPv6 address of RADIUS server
Switch(config)# radius-server key test	Configure shared key of RADIUS server
Switch(config)# end	Exit configuration mode
Switch# show dot1x	Verify and manage dotlx configuration
Switch# show dot1x interface eth-0-25	Verify dotlx configuration on eth-0-25

The steps of configuring switches to enable dotlx on routed ports are as below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# dot1x system-auth-ctrl	Globally enable dotlx authentication control
Switch(config)# interface eth-0-25	Enter interface configuration mode
Switch(config-if)# no switchport	Configure the interface as routed port
Switch(config-if)# ip address 192.168.100.1/24	Configure an IP address on this interface
Switch(config-if)# dot1x port-control auto	Enable dotlx port control on the interface, and permit port access negotiation authentication
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-26	Enter interface configuration mode
Switch(config-if)# no switchport	Configure the interface as routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure an IP address on this interface
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# radius-server host 202.38.100.7	Configure IPv4 address of RADIUS server
Switch(config)# radius-server host 2001:1000::1	Configure IPv6 address of RADIUS server
Switch(config)# radius-server key test	Configure shared key of RADIUS server
Switch(config)# end	Exit configuration mode
Switch# show dot1x	Verify and manage dotlx configuration
Switch# show dot1x interface eth-0-25	Verify dotlx configurations on eth-0-25

The steps of configuring switches to enable force-authorization mode are as below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# dot1x system-auth-ctrl	Globally enable dotlx authentication control
Switch(config)# interface eth-0-25	Enter interface configuration mode
Switch(config-if)# dot1x port-control force-authorized	Enable dotlx port control on the interface, and force-authorized
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# end	Exit configuration mode
Switch# show dot1x	Verify and manage dotlx configuration
Switch# show dot1x interface eth-0-25	Verify dotlx configurations on eth-0-25

The steps of setting optional parameters are as below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# radius-server deadtime 10	Set RADIUS server deadtime
Switch(config)# radius-server retransmit 5	Set maximum RADIUS-to-server retransmits
Switch(config)# radius-server timeout 10	Set RADIUS server timeout
Switch(config)# interface eth-0-25	Enter interface configuration mode
Switch(config-if)# dot1x max-req 5	Specify re-authentication attempts before authorization
Switch(config-if)# dot1x protocol-version 1	Set protocol version
Switch(config-if)# dot1x quiet-period 120	Quiet period in HELD state
Switch(config-if)# dot1x reauthentication	Enable re-authentication on an interface
Switch(config-if)# dot1x timeout re-authperiod 1800	Specify re-authentication period
Switch(config-if)# dot1x timeout server-timeout 60	Set authentication server response timeout
Switch(config-if)# dot1x timeout supp-timeout 60	Specify client response timeout
Switch(config-if)# dot1x timeout tx-period 60	Specify interval of identity information request from client

The detailed steps and parameters of setting server software are as shown in Figures 6-2, 6-3 and 6-4.

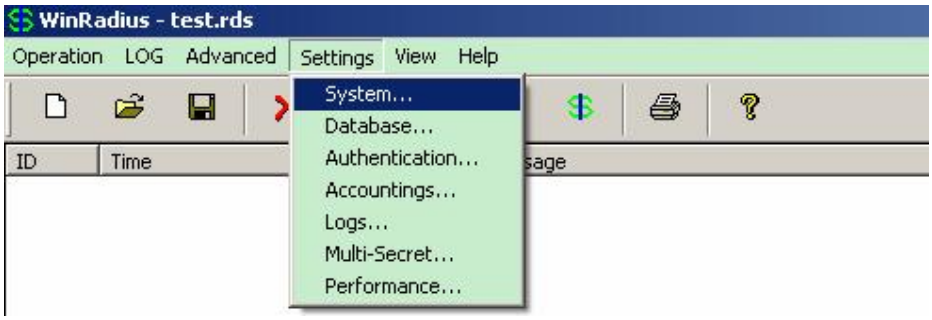


Figure 6-2 Choose Setting -> System

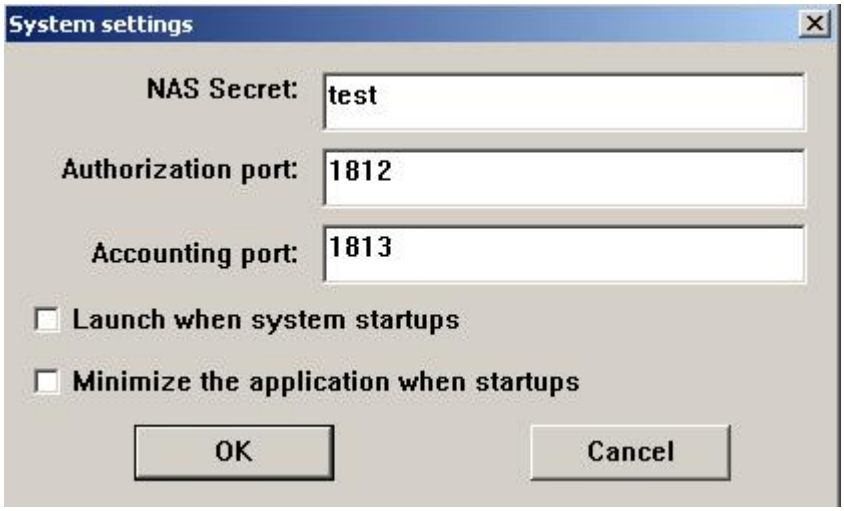


Figure 6-3 Configure password sharing key, authentication port and accounting port of Radius server

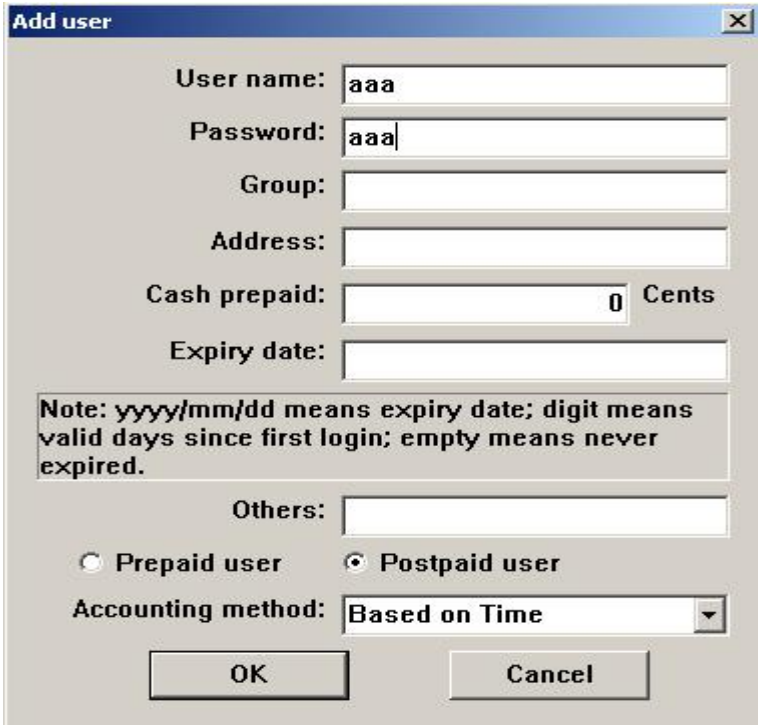


Figure 6-4 Configure user name and password on server client

6.7.4 Command Validation

Use the following steps to display dotlx configuration result.

Switch# show dot1x

802.1X Port-Based Authentication Enabled
RADIUS server address: 2001:1000::1:1812
Next radius message ID: 0
RADIUS server address: 202.38.100.7:1812
Next radius message ID: 0
Switch# show dot1x interface eth-0-25
802.1X info for interface eth-0-25
Supplicant name: aaa
Supplicant address: 0011.11e1.9a3f
portEnabled: true - portControl: Auto
portStatus: Authorized - currentId: 42
reAuthenticate: disabled
reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 41
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false

6.8 Guest VLAN Configuration

6.8.1 Introduction

If a user fails in authentication due to lack of a dedicated authentication client or a low version of client, the port where the user is based will be added to GuestVlan. GuestVlan is accessible without authentication. In the VLAN, users can have actions such as client downloading or updating. After installing or updating the authentication client with these resources, users can go through the authentication procedure normally again, so as to access other network resources. With 802.1x feature enabled and GuestVlan correctly configured, if a device exceeds the maximum times of transmitting EAP-Request/Identity from a port

but receives no response message from the client, the port will be added to GuestVlan. If a user requests authentication in this case and fail, the port continues to remain in guest vlan; if pass, the port will return to th'e VLAN configured by users.

NOTE

Guest VLAN can be configured on Access ports only, and cannot act on layer 3 physical interfaces (routed port)

or trunk ports.

6.8.2 Topology

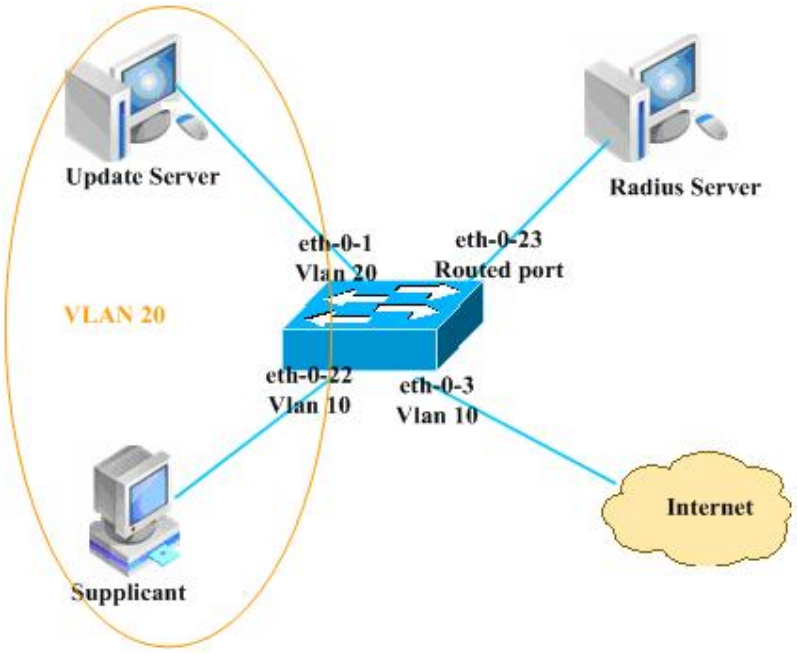


Figure 6-5 Guest VLAN Topology

As shown in Figure 6-5, eth-0-22 is a port with 802.1x enabled and is in VLAN 10. Update server is a server for client downloading and updating in VLAN20. With guest vlan feature enabled on eth-0-22, if a device exceeds the maximum times of transmitting EAP-Request/Identity from a port but receives no response message from the client, the port

will be added to guest VLAN 20. In this case, both clients and the update server are in VLAN 20, and clients can access the update server and download an 802.1x client.

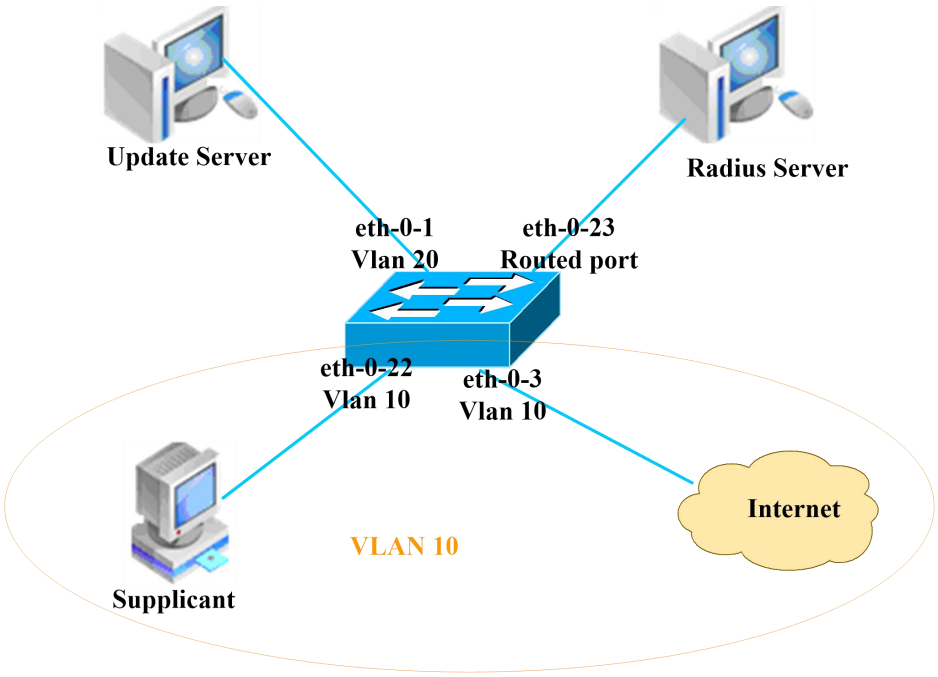


Figure 6-6 Topology of Authentication Success

The uplink port eth-0-23 linking to the radius server is a layer 3 physical port with an IP address of 202.38.100.1, and the radius server address is 202.38.100.7. After authentication success, port eth-0-22 returns to VLAN 10, and clients can access the Internet.

6.8.3 Configuration

Configure Switches

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN configuration mode
Switch(config-vlan)# vlan 10	Create VLAN 10
Switch(config-vlan)# vlan 20	Create VLAN 20
Switch(config-vlan)# exit	Exit VLAN configuration mode
Switch(config)# dot1x system-auth-ctrl	Globally enable dotlx authentication control
Switch(config)# interface eth-0-22	Assign an interface to be configured, and enter interface configuration mode
Switch(config-if)# switchport mode access	Set the interface as access mode
Switch(config-if)# switchport access vlan	Set the port to allow VLAN 10

10	
Switch(config-if)# dot1x port-control auto	Enable dotlx port control on the interface, and permit port access negotiation authentication
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# dot1x guest vlan 20	Configure guest VLAN as VLAN 20
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-23	Assign an interface to be configured, and enter interface configuration mode
Switch(config-if)# no switchport	Configure the interface as routed port
Switch(config-if)# ip address 202.38.100.1/24	Configure an IP address on this interface
Switch(config-if)# no shutdown	Confirm port enabling
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# radius-server host 202.38.100.7	Configure IP address of RADIUS server
Switch(config)# radius-server key test	Configure shared key of RADIUS server
Switch(config)# end	Exit configuration mode
Switch# show dot1x	Verify and manage dotlx configuration
Switch# show dot1x interface eth-0-22	Verify dotlx configuration on eth-0-22

6.8.4 Command Validation

Step 1 The initial state before configuring Guest VLAN is as shown in the screen content of running command “show running-config”.

Switch# show running-config

```
dot1x system-auth-ctrl
radius-server host 202.38.100.7 key test
vlan database
 vlan 10,20
!
interface eth-0-22
 switchport access vlan 10
 dot1x port-control auto
 dot1x guest-vlan 20
!
interface eth-0-23
 no switchport
 ip address 202.38.100.1/24
!
```

```
Switch# show dOt1x interface eth-0-22
802.1X info for interface eth-0-22
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  reAuthenticate: disabled
  reAuthPeriod: 3600
  Guest VLAN:20
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 19
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name          State   STP ID  DSCP    Member ports
                                       (u)-Untagged, (t)-Tagged
=======  ============  =======  =======  =======  ======================
1        default       ACTIVE  0        Disable eth-0-1(u) eth-0-2(u)
                                                  eth-0-3(u) eth-0-4(u)
                                                  eth-0-5(u) eth-0-6(u)
                                                  eth-0-7(u) eth-0-8(u)
                                                  eth-0-9(u) eth-0-10(u)
                                                  eth-0-11(u) eth-0-12(u)
                                                  eth-0-13(u) eth-0-14(u)
                                                  eth-0-15(u) eth-0-16(u)
                                                  eth-0-17(u) eth-0-18(u)
                                                  eth-0-19(u) eth-0-20(u)
                                                  eth-0-21(u) eth-0-24(u)
                                                  eth-0-25(u) eth-0-26(u)
                                                  eth-0-27(u) eth-0-28(u)
                                                  eth-0-29(u) eth-0-30(u)
                                                  eth-0-31(u) eth-0-32(u)
                                                  eth-0-33(u) eth-0-34(u)
                                                  eth-0-35(u) eth-0-36(u)
                                                  eth-0-37(u) eth-0-38(u)
                                                  eth-0-39(u) eth-0-40(u)
                                                  eth-0-41(u) eth-0-42(u)
                                                  eth-0-43(u) eth-0-44(u)
                                                  eth-0-45(u) eth-0-46(u)
                                                  eth-0-47(u) eth-0-48(u)
10       VLAN0010      ACTIVE  0        Disable eth-0-22(u)
20       VLAN0020      ACTIVE  0        Disable
```

Step 2 The status information of Guest VLAN client is as shown in the screen echo information below.

Switch# show dot1x interface eth-0-22

```
802.1X info for interface eth-0-22
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
```

```
 Guest VLAN:20(Port Authorized by guest vlan)
 abort:F fail:F start:F timeout:F success:F
 PAE: state: Connecting - portMode: Auto
 PAE: reAuthCount: 2 - rxRespId: 0
 PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
 BE: state: Idle - reqCount: 0 - idFromServer: 19
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in - operControlledDirections: in
 CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name          State   STP ID  DSCP    Member ports
                                 (u)-Untagged, (t)-Tagged
======= ================ ======== ======= ======= ========================
1      default         ACTIVE  0      Disable eth-0-1(u) eth-0-2(u)
                                             eth-0-3(u) eth-0-4(u)
                                             eth-0-5(u) eth-0-6(u)
                                             eth-0-7(u) eth-0-8(u)
                                             eth-0-9(u) eth-0-10(u)
                                             eth-0-11(u) eth-0-12(u)
                                             eth-0-13(u) eth-0-14(u)
                                             eth-0-15(u) eth-0-16(u)
                                             eth-0-17(u) eth-0-18(u)
                                             eth-0-19(u) eth-0-20(u)
                                             eth-0-21(u) eth-0-24(u)
                                             eth-0-25(u) eth-0-26(u)
                                             eth-0-27(u) eth-0-28(u)
                                             eth-0-29(u) eth-0-30(u)
                                             eth-0-31(u) eth-0-32(u)
                                             eth-0-33(u) eth-0-34(u)
                                             eth-0-35(u) eth-0-36(u)
                                             eth-0-37(u) eth-0-38(u)
                                             eth-0-39(u) eth-0-40(u)
                                             eth-0-41(u) eth-0-42(u)
                                             eth-0-43(u) eth-0-44(u)
                                             eth-0-45(u) eth-0-46(u)
                                             eth-0-47(u) eth-0-48(u)
10     VLAN0010        ACTIVE  0      Disable
20     VLAN0020        ACTIVE  0      Disable eth-0-22(u)
```

Step 3 Client is authenticated

Switch# show dot1x interface eth-0-22

```
802.1X info for interface eth-0-22
 Supplicant name: ychen
 Supplicant address: ae38.3288.f046
 portEnabled: true - portControl: Auto
 portStatus: Authorized - currentId: 6
 reAuthenticate: disabled
 reAuthPeriod: 3600
 Guest VLAN:20
 abort:F fail:F start:F timeout:F success:T
 PAE: state: Authenticated - portMode: Auto
 PAE: reAuthCount: 0 - rxRespId: 0
```

```
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 5
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name          State   STP ID  DSCP    Member ports
                                 (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1      default        ACTIVE  0      Disable eth-0-1(u) eth-0-2(u)
                                              eth-0-3(u) eth-0-4(u)
                                               eth-0-5(u) eth-0-6(u)
                                               eth-0-7(u) eth-0-8(u)
                                               eth-0-9(u) eth-0-10(u)
                                               eth-0-11(u) eth-0-12(u)
                                               eth-0-13(u) eth-0-14(u)
                                               eth-0-15(u) eth-0-16(u)
                                               eth-0-17(u) eth-0-18(u)
                                               eth-0-19(u) eth-0-20(u)
                                               eth-0-21(u) eth-0-24(u)
                                               eth-0-25(u) eth-0-26(u)
                                               eth-0-27(u) eth-0-28(u)
                                               eth-0-29(u) eth-0-30(u)
                                               eth-0-31(u) eth-0-32(u)
                                               eth-0-33(u) eth-0-34(u)
                                               eth-0-35(u) eth-0-36(u)
                                               eth-0-37(u) eth-0-38(u)
                                               eth-0-39(u) eth-0-40(u)
                                               eth-0-41(u) eth-0-42(u)
                                               eth-0-43(u) eth-0-44(u)
                                               eth-0-45(u) eth-0-46(u)
                                               eth-0-47(u) eth-0-48(u)
10     VLAN0010       ACTIVE  0      Disable eth-0-22(u)
20     VLAN0020       ACTIVE  0      Disable
```

Switch# show dot1x

```
802.1X Port-Based Authentication Enabled
  RADIUS server address: 202.38.100.7:1812
  Next radius message ID: 0
Switch# show dot1x statistics
=====================================
802.1X statistics for interface eth-0-22
  EAPOL Frames Rx: 52 - EAPOL Frames Tx: 4270
  EAPOL Start Frames Rx: 18 - EAPOL Logoff Frames Rx: 2
  EAP Rsp/Id Frames Rx: 29 - EAP Response Frames Rx: 3
  EAP Req/Id Frames Tx: 3196 - EAP Request Frames Tx: 3
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 2 - EAPOL Last Frame Src: ae38.3288.f046
```

6.9 ARP Inspection Configuration

6.9.1 Introduction

By default, all ARP messages will pass through switches in accordance with the rules. Users can enable the ARP Inspection feature to monitor ARP messages; the feature can filter invalid messages by means of validity check of ARP messages or permit or discard specific ARP messages by setting rules, so as to enhance system security and inhibit ARP message attack to some extent.

ARP inspection is a security feature for inspecting ARP messages in the network, which can act to inspect logs and discard ARP messages bound by invalid IP or MAC. This can protect the network from human attack. ARP inspection guarantees that only invalid ARP requests and responses are executed. The actions executed by switches include: intercepting all ARP requests and responses on untrusted ports.

All the inspected messages must be checked for validity before updating of local ARP cache or forwarding messages to specific destination addresses.

Discarding invalid ARP messages: ARP inspection is to determine the validity of an ARP message based on the binding of the existing DHCP snooping database with valid IPs or MACs. On a trusted port, switches forward messages without inspection. On an untrusted port, switches only forward valid messages.

6.9.2 Terms

The below briefs the terms and concepts related to ARP Inspection:

DHCP Snooping

DHCP snooping is a security feature for executing firewall function between untrusted host and trusted DHCP server. The feature establishes and maintains DHCP snooping databases, and the databases contain the information of untrusted host renting IP addresses.

Address Resolution Protocol (ARP)

ARP provides IP communication in layer 2 broadcast domain by mapping IP addresses and MAC addresses. For example, if host B intends to send information to host A but hasn't acquired the MAC address of host A, then host B generates a broadcast message to all hosts in the broadcast domain to request the MAC address of host A. All hosts in the broadcast domain receive the ARP request, and host A returns its MAC address.

6.9.3 Configuration

Create VLAN

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Configure VLAN database
Switch(config-vlan)# vlan 2	Create VLAN 2

Switch(config-vlan)# exit	Exit VLAN configuration mode
Switch(config)# exit	Exit global configuration mode

Add An Interface to VLAN

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode, and start configuring interface eth-0-1
Switch(config-if)# switchport access vlan 2	Add the interface to VLAN2
Switch(config-if)# interface eth-0-2	Start configuring interface eth-0-2
Switch(config-if)# switchport access vlan 2	Add the interface to vlan 2
Switch(config-if)# interface eth-0-3	Start configuring interface eth-0-3
Switch(config-if)# switchport access vlan 2	Add the interface to VLAN 2
Switch(config-if)# interface eth-0-4	Start configuring eth-0-4
Switch(config-if)# switchport access vlan 2	Add the interface to VLAN 2
Switch(config-if)# exit	Exit interface configuration mode

Configure ARP Inspection

Switch(config)# interface eth-0-1	Enter interface configuration mode, and start configuring interface eth-0-1
Switch(config-if)# ip arp inspection trust	Configure the interface as trust (usually configure the interfaces of interconnected switches as trust
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# ip arp inspection vlan 2	Enable ARP inspection on VLAN2
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog	Enable showing ARP inspection match log on VLAN2
Switch(config)# ip arp inspection validate src-mac ip dst-mac	Validate source MAC address, IP and destination MAC address in ARP message

Add ARP ACL

Switch(config)# arp access-list test	Create ARP access-list of test
Switch(config-arp-acl)# deny request ip host 1.1.1.1 mac any	Add an ACL item to deny 1.1.1.1ARP request
Switch(config-arp-acl)# exit	Exit ARP ACL configuration mode
Switch(config)# ip arp inspection filter test vlan 2	Enable ARP ACL on VLAN2
Switch(config)# exit	Exit global configuration mode

6.9.4 Command Validation

The steps of validating ARP inspection configuration on switches are as below.

Switch# show ip arp inspection

```
Source Mac Validation      : Enabled
Destination Mac Validation  : Enabled
IP Address Validation       : Enabled
Vlan    Configuration    ACL Match    Static ACL
============================================================
2       enabled          test
Vlan    ACL Logging    DHCP Logging
============================================================
2       deny             deny
Vlan    Forwarded      Dropped    DHCP Drops    ACL Drops
============================================================
2       0              0          0             0
Vlan    DHCP Permits    ACL Permits    Source MAC Failures
============================================================
2       0               0              0
Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
============================================================
2      0                   0                        0
```

View ARP Inspection log information on switch:

Switch# show ip arp inspection log

```
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
```

```
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
```

6.10 DHCP Snooping Configuration

6.10.1 Introduction

DHCP Snooping is a security feature like firewall action between untrusted host and trusted DHCP server. DHCP Snooping executes the following actions:

- Validating DHCP messages are from an untrusted source and filtering out invalid messages.
- Establishing and maintaining DHCP Snooping binding databases, which contain the IP address information rented by untrusted hosts.
- Validating subsequent requests from untrusted hosts based on the DHCP Snooping binding databases.
- Other security functions such as dynamic ARP monitoring. Also can use the information stored in the DHCP Snooping binding databases. Enable the DHCP Snooping feature based on VLAN, which is inactive on all VLANs by default. You can use this feature in an individual VLAN or within a VLAN range. The DHCP Snooping feature is realized in software, and all DHCP messages are intercepted in chip and directly sent to the CPU for processing.

6.10.2 Configuration

Configure VLAN

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Configure VLAN database
Switch(config-vlan)# vlan 12	Create VLAN 12
Switch(config-vlan)# exit	Exit global configuration mode

Configure Interface Eth-0-12

Switch(config)# interface eth-0-12	Enter interface configuration mode
Switch(config-if)# switchport	Set as switch port
Switch(config-if)# switchport access vlan 12	Add the interface to VLAN 12
Switch(config-if)# dhcp snooping trust	Configure the interface as trust
Switch(config-if)# no shutdown	Enable the interface

Switch(config-if)# exit	Exit global configuration mode

Configure Interface Eth-0-11

Switch(config)# interface eth-0-11	Enter interface configuration mode
Switch(config-if)# switchport	Set as switch port
Switch(config-if)# switchport access vlan 12	Add the interface to VLAN 12
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit global configuration mode

Configure VLAN12 Interface

Switch(config)# interface vlan 12	Enter interface configuration mode
Switch(config-if)# ip address 12.1.1.1/24	Set VLAN 12 IP address
Switch(config-if)# exit	Exit interface configuration mode

Configure DHCP Feature

Switch(config)# dhcp snooping verify mac-address	Check the header MAC address of the request message from DHCP user for validity

Enable Global DHCP Snooping Feature

Switch(config)# service dhcp enable	Enable dhcp service
Switch(config)# dhcp snooping	Enable dhcp snooping feature
Switch(config)# dhcp snooping vlan 12	Enable dhcp snooping feature on VLAN 12

6.10.3 Command Validation

Step 1 The steps of checking the interface configuration for validity are as below.

Switch(config)# show running-config interface eth-0-12

!

```
interface eth-0-12
 dhcp snooping trust
 switchport access vlan 12
!
Switch(config)# show running-config interface eth-0-11
!
interface eth-0-11
 switchport access vlan 12
!
```

Step 2 Use the following command to check DHCP service status.

Switch# show services

```
Networking services configuration:
Service Name        Status
============================================================
dhcp                enable
```

Step 3 Use the following command to print dhcp snooping configuration and check the current configuration.

Switch# show dhcp snooping config

```
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): disable
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 12
```

Step 4 Use the following command to check dhcp snooping statistics.

Switch# show dhcp snooping statistics

```
DHCP snooping statistics:
============================================================
DHCP packets                    17
BOOTP packets                   0
Packets forwarded               30
Packets invalid                 0
Packets MAC address verify failed  0
Packets dropped                 0
```

Step 5 Use the following command to display dhcp snooping biding information.

Switch# show dhcp snooping binding all

```
DHCP snooping binding table:
VLAN MAC Address    Interface  Lease(s)   IP Address
============================================================
12   0016.76a1.7ed9 eth-0-11   691190     12.1.1.65
```

6.11 IP Source Guard Configuration

6.11.1 Introduction

The IP Source Guard binding function allows filtration control over messages forwarded via ports to deny messages with an illegal IP address or MAC address, so as to enhance port security. Ports will process the received messages based on reference to the IP Source Guard binding table entries:

Step 1 For the IP+Port binding table entries, if the source IP address in the message is identical with that recorded in the binding table entries, the port will forward the message; if not, the port will discard the message.

Step 2 For the IP+Port+MAC binding table entries, if the source MAC address and source IP address in the message are identical with that recorded in the binding table entries, the port will forward the message; if not, the port will discard the message.

Step 3 For the IP+Port+MAC+VLAN binding table entries, if the source MAC address, source IP address and VLAN in the message are identical with that recorded in the binding table entries, the port will forward the message; if not, the port will discard the message.

6.11.2 Terms

The below briefs the terms and concepts related to IP source guard.

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is a client/server protocol that will automatically provide an IP address and other related information such as subnet mask and default gateway to an IP host.

DHCP Snooping

DHCP Snooping is a security feature like firewall action between untrusted host and trusted DHCP server. This feature establishes and maintains DHCP Snooping binding databases, which contain the IP address information rented by untrusted hosts.

ACL

Access control list.

6.11.3 Configuration

Configure VLAN Information

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 3	Create VLAN3
Switch(config-vlan)# exit	Exit VLAN mode

Switch(config)# interface eth-0-16	Enter interface mode
Switch(config-if)# switchport	Set the interface as layer2 interface
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# switchport access vlan 3	Set the interface to belong to VLAN3
Switch(config-if)# exit	Exit interface mode

Configure IP Source Guard

Switch(config)# ip source maximal binding number per-port 15	Set maximum binding number per port as 15
Switch(config)# ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	Configure IP Source Guard binding table entries
Switch(config)# interface eth-0-16	Enter interface mode
Switch(config-if)# ip verify source ip	Enable IP+Port binding inspection under the interface
Switch(config-if)# exit	Exit interface mode

Delete Configuration

Switch(config)# no ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	Delete an individual IP Source Guard binding table entry
Switch(config)# no ip source binding entries interface eth-0-16	Delete all eth-0-16 binding table entries
Switch(config)# no ip source binding entries vlan 3	Delete all VLAN 3 binding table entries
Switch(config)# no ip source binding entries	Clear all binding table entries

6.11.4 Command Validation

Switch#show running-config interface eth-0-16

```
!
interface eth-0-16
 ip verify source ip
 switchport access vlan 3
```

6.12 Private Vlan Configuration

6.12.1 Introduction

Private vlan attribute refers to isolation and intercommunication of layer 2 traffic within a same vlan.

Can provide flexible networking methods as needed.

6.12.2 Topology

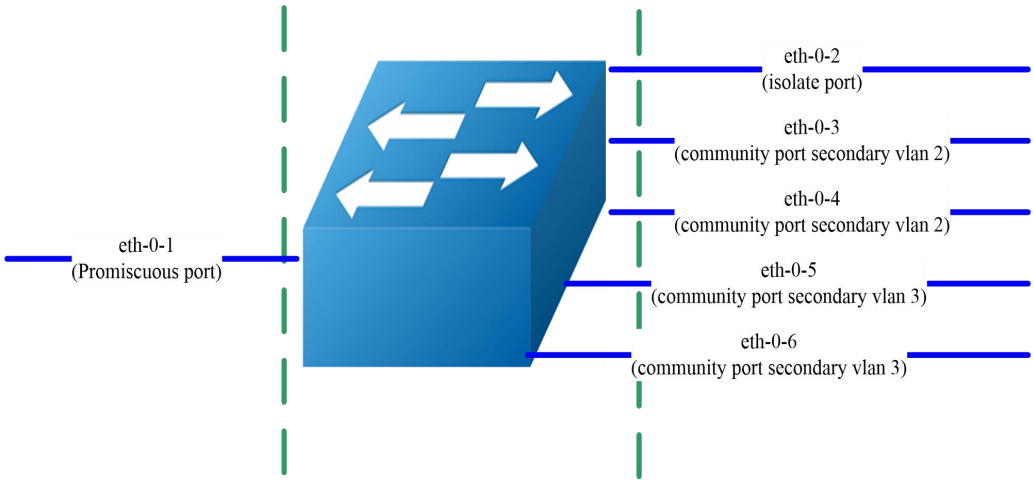


Figure 6-7 Private Vlan Basic Topological Graph

All ports are in a same private vlan.

Port 1 is a hybrid port that can intercommunicate with all other ports in the same private vlan

Port 2 is an isolate port that is mutually isolated from all other ports except for the hybrid port (Port 1)in the same private vlan

Ports 3 and 4 are interconnected ports and belong to sub vlan 2. Ports 3 and 4 interconnect with each other and with the hybrid port. They are mutually isolated from other ports in the same private vlan.

Ports 5 and 6 are interconnected ports and belong to sub vlan 3. Ports 5 and 6 interconnect with each other and with the hybrid port. They are mutually isolated from other ports in the same private vlan.

6.12.3 Configuration

Switches Configuration.

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN mode
Switch(config-vlan)# vlan 2	Create vlan 2

Switch (config-vlan)# quit	Exit vlan mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch (config-if)# switchport mode private-vlan promiscuous	Configure private vlan mode as hybrid port
Switch (config-if)# switchport private-vlan 2	Configure primary vlan 2
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Configure private vlan mode as host port
Switch (config-if)# switchport private-vlan 2 isolate	Configure private vlan mode as isolate port, and configure primary vlan as 2
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-3	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Configure private vlan mode as host port
Switch (config-if)# switchport private-vlan 2 community-vlan 2	Configure private vlan mode as interconnected port, and configure primary vlan as 2, and sub vlan as 2
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-4	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Configure private vlan mode as host port
Switch (config-if)# switchport private-vlan 2 community-vlan 2	Configure private vlan mode as isolate port, and configure primary vlan as 2
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-5	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Configure private vlan mode as host port
Switch (config-if)# switchport private-vlan 2 community-vlan 3	Configure private vlan mode as isolate port, and configure primary vlan as 3
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-6	Enter interface mode
Switch (config-if)# switchport mode private-vlan host	Configure private vlan mode as host port
Switch (config-if)# switchport private-vlan 2	Configure private vlan mode as isolate port,

community-vlan 3	and configure primary vlan as 3
Switch (config-if)# quit	Exit interface mode

6.12.4 Command Validation

The show results are as below:

switch # show private-vlan

Primary Secondary Type Ports

2	N/A	promiscuous	eth-0-1	
2	N/A	isloate	eth-0-2	
2	2	community	eth-0-3	eth-0-4
2	3	community	eth-0-5	eth-0-6

6.13 AAA Configuration

6.13.1 Introduction

The system can authenticate users accessing the network and network services by means of AAA authentication. RADIUS authentication is one of AAA authentication methods. RADIUS is a distributed client/server system for preventing unauthorized access to guarantee network security. RADIUS is a protocol widely applied in the network environment. It is usually applied for embedded network devices such as router, modem server, switch, etc. RADIUS clients generally run on routers and switches supporting RADIUS. Clients send authentication requests to the RADIUS server. RADIUS server contains all user authentication and network service access information.

6.13.2 Topology

The network topology of RADIUS is as below.

A PC acts as RADIUS server, configured with a network card 1.1.1.2/24.

Interface eth-0-23 of the switch is set with an IP address of 1.1.1.1/24. The management port of the switch is set with an IP address of 10.10.29.215, and the PC connected to the switch with an IP address of 10.10.29.10.

Figure 6-8 RADIUS Topology

6.13.3 Configuration

Configure AAA

Switch# configure terminal	Enter global configuration mode
Switch(config)# aaa new-model	Enable AAA protocol
Switch(config)# aaa authentication login radius-login radius local	Set AAA authentication mode
Switch(config)# radius-server host 1.1.1.2 auth-port 1819 key keyname	Configure RADIUS server parameters
Switch(config)# radius-server host 2001:1000::1 auth-port 1819 key keyname	(Optional) Configure RADIUS server parameters
Switch(config)# interface eth-0-23	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address
Switch (config-if)# quit	Exit interface mode
Switch(config)# line vty 0 7	Enter VTY mode
Switch(config-line)#login authentication radius-login Switch(config-line)#privilege level 4 Switch(config-line)#no line-password	Configuration authentication method

Configure PC and WinRADIUS

Step 1 Configure IP addresses following Figure 6-9.

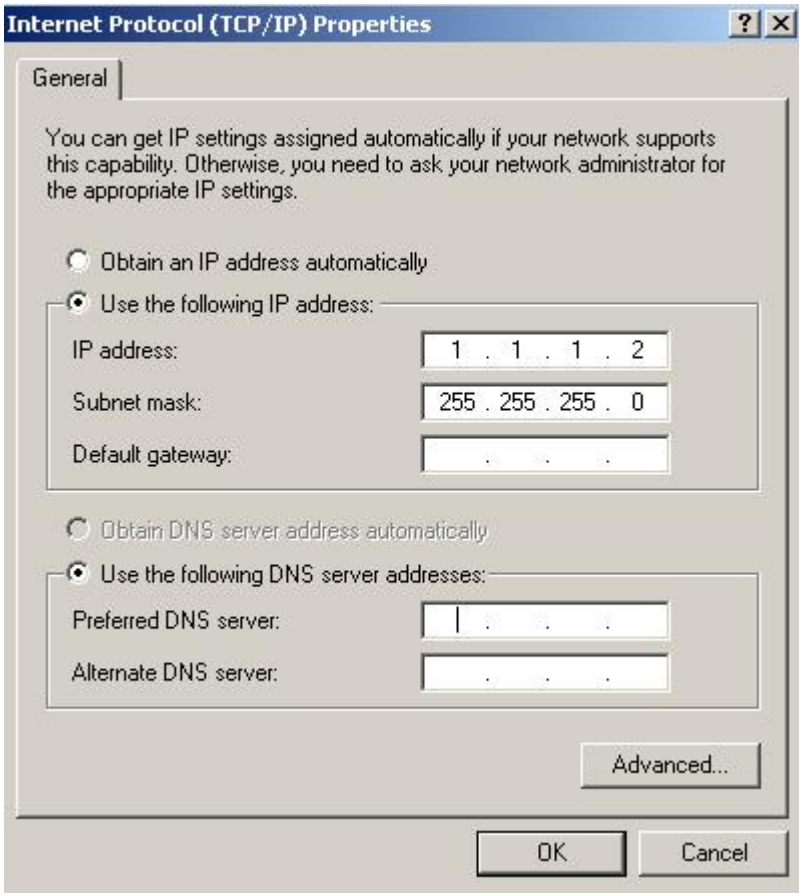


Figure 6-9 Configure IP addresses

Step 2 Test the connectivity between client and server following Figure 6-10.

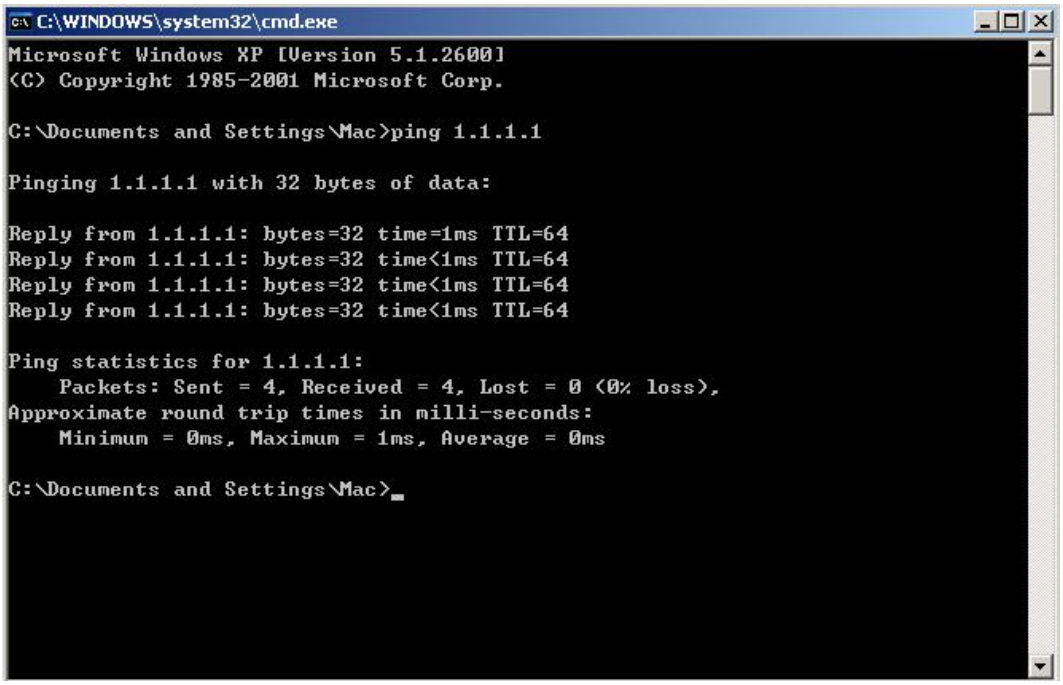


Figure 6-10 Connectivity check result

Step 3 Open server software following Figure 6-11.

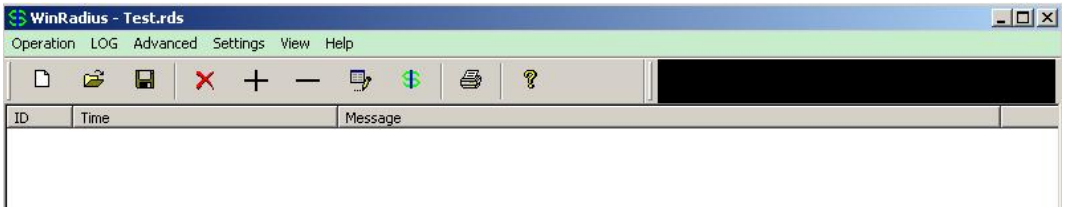


Figure 6-11 Open server software

Step 4 Complete system settings following Figure 6-12.

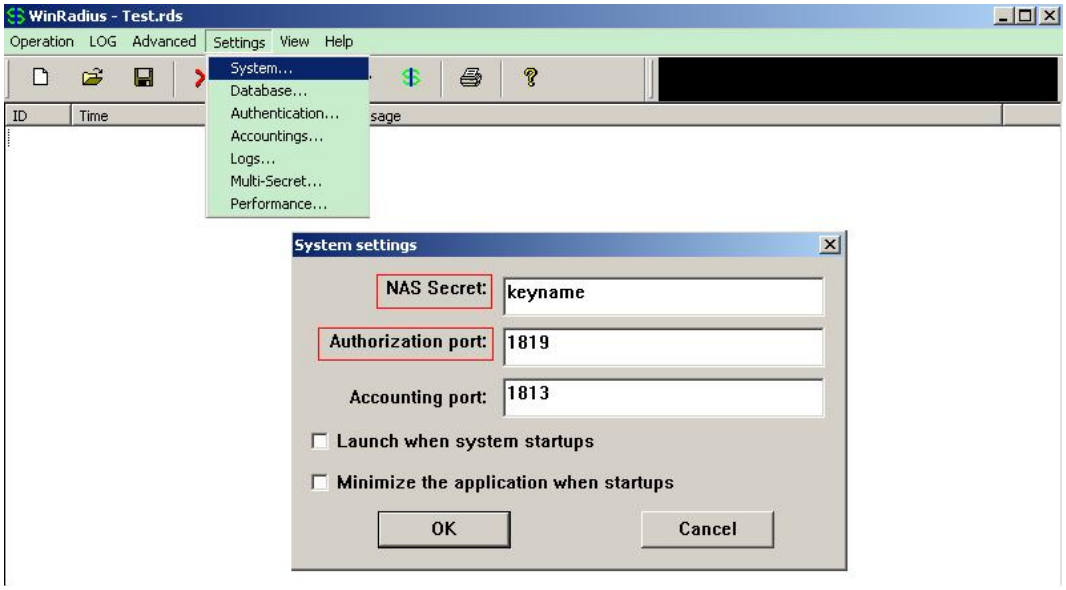


Figure 6-12 System Configuration

Step 5 Add user name and password following the steps and parameters as shown in Figure 6-13.

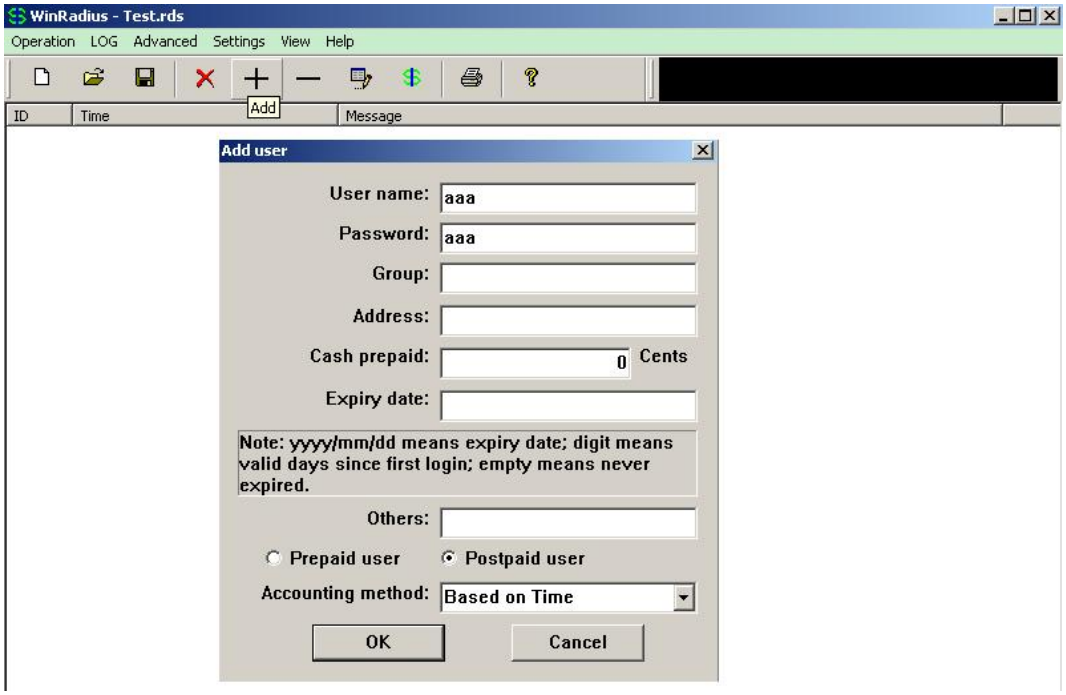


Figure 6-13 Add user name and password

Step 6 Use command “ping” to check the connectivity following Figure 6-14.

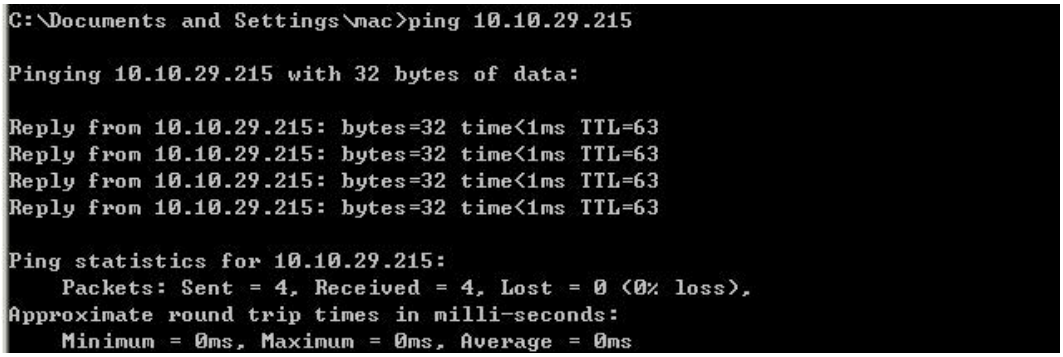


Figure 6-14 Ping check result

6.13.4 Command Validation

Use command “show” to check the working state of switches.

Switch# show aaa status

aaa stats:
Authentication enable

Use command “show” to display key information in switches.

Switch# show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN
Name = default state = ALIVE : local
Name = radius-login state = ALIVE : radius local

6.13.5 Show Results

Conduct Telnet test. The result of Telnet connection test is similar to Figure 6-15 if the configuration is correct.

Figure 6-15 Telnet Connection Test

NOTE

Be sure to enable the RADIUS authentication function.

Confirm the correctness of cable connection.

If the switch fails to complete RADIUS authentication, you can use the command below to check out the system log:

Switch# show logging buffer

6.14 TACACS+Configuration

6.14.1 Introduction

The system can authenticate users accessing the network and network services by means of AAA authentication. TACACS+authentication is one of AAA authentication methods. TACACS+ is a distributed client/server system for preventing unauthorized access to guarantee network security. TACACS+ is a protocol widely applied in the network environment. It is usually applied for embedded network devices that support TACACS+, such as router, modem server, switch, etc. Clients send authentication requests to TACACS+ server. TACACS+ server contains all user authentication and network service access information.

6.14.2 Topology

The network topology of TACACS+ is as below. A PC acts as TACACS+ server, configured with a network card 1.1.1.2/24. Interface eth-0-23 of the switch is set with an IP address of 1.1.1.1/24. The management port of the switch is set with an IP address of 10.10.29.215, and the PC connected to the switch (in-band management only) with an IP address of 10.10.29.10.

Figure 6-16 TACACS+ Topology

6.14.3 Configuration

Configure AAA and TACACS+

Switch# configure terminal	Enter global configuration mode
Switch(config)# aaa new-model	Enable AAA protocol
Switch(config)# aaa authentication login tac-login tacacs-plus local	Set AAA authentication mode
Switch(config)# aaa authorization exec default tacacs-plus	Set AAA authorization mode
Switch(config)# aaa accounting exec default start-stop tacacs-plus	Set AAA EXEC accounting

Switch(config)# aaa accounting commands default tacacs-plus	Set AAA command line accounting
Switch(config)# tacacs-server host 1.1.1.2 port 123 key keyname	Configure IP address, authentication and password of TACACS+ server
Switch(config)# interface eth-0-23	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 1.1.1.1/24	Configure an IP address
Switch (config-if)# quit	Exit interface mode
Switch(config)# line vty 0 7	Enter VTY mode
Switch(config-line)#login authentication tac-login Switch(config-line)#privilege level 4 Switch(config-line)#no line-password	Configuration authentication method

6.14.4 Configure TACACS+ server

Step 1 Download TACACS+ server code, DEVEL.201105261843.tar.bz2.

Step 2 Compile TACACS+ server code.

Step 3 Change the configuration file by adding user name and password.

```
#!../obj.linux-2.6.9-89.29.1.elsmp-x86_64/tac_plus
id = spawnd {
        listen = { port = 49 }
        spawn = {
                instances min = 1
                instances max = 10
        }
        background = no
}
        user = aaa {
                password = clear bbb
                member = guest
        }
```

Step 4 Run TACACS+ server program.

```
[disciple: ~]$ ./tac_plus ./tac_plus.cfg.in -d 1
```

Step 5 Use the “Ping” command to check connection result.

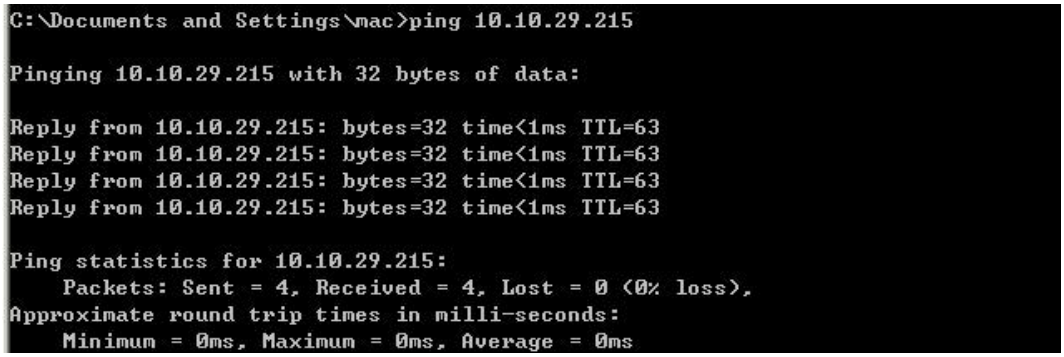


Figure 6-17 Connectiion result

6.14.5 Command Validation

Use the “show authentication status” command to check the configuration.

Switch# show aaa status

aaa stats:
Authentication enable

Use the “show aaa method-lists authentication” command to check AAA configuration.

Switch# show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN
Name = default state = ALIVE : local
Name = tac-login state = ALIVE : tacacs-plus local

6.14.6 Show Results

Conduct Telnet test. The result of Telnet connection test is similar to Figure 6-18 if the configuration is correct.

Figure 6-18 Telnet Test Result

6.15 Port-Isolate Configuration

6.15.1 Introduction

That the ports of different users belong to a same VLAN but are not interconnected with each other can be realized via the Port-Isolated feature. This helps enhance network security, provide flexible networking methods, and save a large amount of VLAN resources.

6.15.2 Topology

Figure 6-19 shows basic topology for port-isolate.

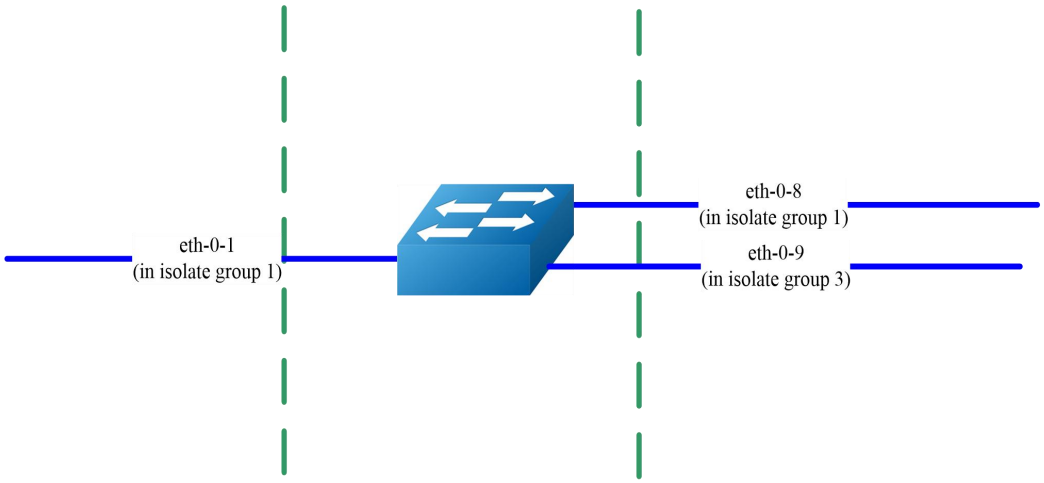


Figure 6-19 Basic topology for port-isolate

Ports 1 and 8 both are in isolate group1, so they cannot interconnect with each other.

Ports 9 is in isolate group 3, so it can interconnect with Ports 1 and 8.

6.15.3 Configuration

Switches Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# port-isolate mode l2	Set port-isolate mode
Switch(config-if)# interface eth-0-1	Enter interface mode
Switch(config-if)# port-isolate group 1	Set the interface to belong to port-isolate group 1
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-8	Enter interface mode
Switch(config-if)# port-isolate group 1	Set the interface to belong to port-isolate group 1
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# port-isolate group 3	Set the interface to belong to port-isolate group 3
Switch(config-if)# exit	Exit interface mode
Switch(config)# end	Exit configuration mode
Switch# show port-isolate	Show port-isolate configuration

6.15.4 Command Validation

Use the following command to show port-isolate configuration.

```
switch# show port-isolate
------------------------------------------------------------------
 Port Isolate Groups:
------------------------------------------------------------------
 Groups ID: 1
eth-0-1，eth-0-8
------------------------------------------------------------------
Groups ID: 3
eth-0-9
------------------------------------------------------------------
```

6.16 DDoS Defense Configuration

6.16.1 Introduction

DDos is short for distributed denial-of-service attack, which is derived from DoS (denial-of-service) attack. Its working principle is to consume excessive service resources utilizing reasonable service requests to enable the server to process instructions from valid users. DDoS attack refers to utilizing multiple attackers in different locations to launch an attack against one or more objects simultaneously, or that one or more attackers have controlled multiple machines (puppet) in different locations and utilize these machines to launch an attack against the victim simultaneously. DDoS attack will lead to service interruption due to network resource waste, link bandwidth congestion, or exhaustion of server resources.

The DDoS defense feature can protect switches from attacks of the following types and intercept the corresponding data packets:

- ICMP flooding: This type of attack is realized by sending bulk ICMP packets to the object IP to consume bandwidth, so that valid messages cannot reach the destination.
- Smurf attack: Attackers uses the address of the victim computer to send ICMP echo requests to a broadcast address, the potential computers in the broadcast network will make responses, and a large amount of responses will be sent to the victim computer. The consequences of this attack type is same with that of ICMP flooding, but the former is more secretive.
- SYN flooding: This type of attack is launched by deliberately hacking tcp three-way handshaking and opening plenty of TCP/IP links. IP cheating is utilized to send SYN requests seeming to be valid to the victim system. In fact, however, the source address doesn't exist or is not online at that time, so that the response ACK message cannot reach the destination. The victim system is filled with plenty of half-open connections to exhaust the resources, while legal connections cannot get a response.
- UDP flooding: This type of attack is realized by sending bulk UDP packets to the object to occupy bandwidth and consume resources.
- Fraggle attack: It is a variant of smurf. Considering the strict inspection over ICMP packets of firewall, it sends UDP packets rather than ICMP request packets to broadcast addresses.
- Small-packet attack: It refers to sending bulk small packets to the victim system to consume the system resources.
- Bad mac intercept: Message attack by setting the destination MAC address equal to the source MAC address.
- Bad ip equal: Message attack by setting the destination IP address equal to the source IP address.

6.16.2 Configuration

Configure ICMP Flooding Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip icmp intercept maxcount 100	Enable ICMP flooding detection, and set the maximum ICMP packet count per

	second as 100
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure UDP Flooding Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip udp intercept maxcount 100	Enable UDP flooding detection, and set the maximum UDP packet count per second as 100
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure Smurf Attack Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip smurf intercept	Enable smurf attack detection
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure SYN Flooding Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip tcp intercept maxcount 100	Enable SYN flooding detection, and set the maximum TCP SYN packet count per second as 100
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure Fraggle Attack Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip fraggle intercept	Enable Fraggle attack detection
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure Small-packet Attack Defense

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip small-packet intercept maxlength 32	Enable small-packet attack detection, and set the minimum receiving IP message length as 32 bytes
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure Same IP Message Filtering

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip ipeq intercept	Enable detecting message attack in the case of destination IP address equal to source IP address
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

Configure Same MAC Message Filtering

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip maceq intercept	Enable detecting message attack in the case of destination MAC address equal to source MAC address
Switch(config)# end	Exit global configuration mode
Switch# show ip-intercept config	Show current DDoS defense configuration

6.16.3 Command Validation

Switch# show ip-intercept config

```
Current DDoS Prevent configuration:
============================================================
ICMP Flood Intercept            :Enable  Maxcount:100
UDP Flood Intercept             :Enable  Maxcount:100
SYN Flood Intercept             :Enable  Maxcount:100
Small-packet Attack Intercept   :Enable  Packet Length:32
Sumrf Attack Intercept          :Enable
Fraggle Attack Intercept        :Disable
MAC Equal Intercept             :Enable
IP Equal Intercept              :Enable
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
============================================================
Resist Small-packet Attack packets number   : 65
Resist ICMP Flood packets number            : 0
Resist Smurf Attack packets number          : 0
Resist SYN Flood packets number             : 0
Resist UDP Flood packets number             : 0
```

6.17 Key Chain Configuration

6.17.1 Introduction

Key chain is a universal authentication method that applies for the entities required to share keys to complete authentication by exchanging keys before building up mutual trust. This authentication method is usually used in routing protocols and network applications for enhancing communication security between peer pairs.

Key chain provides a security mechanism contains key control and a lifecycle-based rollover method, by which a chain of keys are linked together via lifecycle and arranged in the key chain according to the serial number. The working principle of key chain is to compare the keys in the chain one by one, and authentication will be completed once the right key is located.

To make use of lifecycle, the valid time of keys must be defined before using of the key chain, and it is better to use multiple valid keys once to guarantee the stability.

6.17.2 Configuration

Configure Key Chain

Switch# configure terminal	Enter global configuration mode
Switch(config)# key chain test	Create a key chain named test, and enter key chain configuration mode

Switch(config-keychain)# key 1	Create a key with ID 1, and enter key configuration mode
Switch(config-keychain-key)# key-string ##test_keystring_1##	Configure key string
Switch(config-keychain-key)# accept-lifetime 0:0:1 1 jan 2012 infinite	Configure key accept lifetime
Switch(config-keychain)# key 2	Create a key with ID 2, and enter key configuration mode
Switch(config-keychain-key)# key-string ##test_keystring_2##	Configure key string
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite	Configure key send lifetime

6.17.3 Command Validation

Use command “show key chain” in privilege mode to show key chain configuration.

Switch # show key chain

```
key chain test:
   key 1 -- text "key-string ##test_keystring_1##"
     accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
     send-lifetime <always valid> - <always valid> [valid now]
   key 2 -- text "key-string ##test_keystring_2##"
     accept-lifetime <always valid> - <always valid> [valid now]
     send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

6.18 Port-Block Configuration

6.18.1 Introduction

By default, port flooding messages have no destination MAC address. If these messages are transmitted to protected ports, safety problems may arise. Any unicast or multicast with an unknown or known destination MAC address can be prevented from being transmitted to other ports by port-block.

6.18.2 Configuration

Configure Key Chain

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# port-block	Set port-block against unicast with an

unknown-unicast	unknown MAC address
Switch(config-if)# end	Exit global configuration mode
Switch# show port-block interface eth-0-1	Show port-block configuration information

6.18.3 Command Validation

Configure port-block under an interface, and show the configuration information:

```
Switch # show port-block interface eth-0-1
 Known unicast blocked: Enabled
 Known multicast blocked: Disabled
 Unknown unicast blocked: Disabled
 Unknown multicast blocked: Disabled
 Broadcast blocked: Disabled
```

7 IP Service Configuration Guide

7.1 ARP Configuration

7.1.1 Introduction

ARP (Address resolution protocol) is designed to resolve IP addresses at network layer into physical addresses (MAC address) at data link layer.

ARP caches IP and MAC addresses mapping. If the address mapping requested by an interface is not in the cache, the device will cache the received message and broadcast an address request in the appropriate subnet, and generate a new address mapping and transmit the cached message if getting a response. ARP will cache up to one message while waiting for an address mapping response , and only the most recent message will be saved. If the destination port fails to respond after three requests, the host is regarded to have broken down, and a related error message will be returned. If the destination port stops sending messages for a period (usually one hour), the host is regarded likely to have broken down, and the few requests (usually 6, consisting 3 unicast requests and 3 broadcast requests) before deleting of the ARP table entries will be sent to the host.

ARP table entries can be manually added, deleted or modified. Manually added table entries are perpetual.

7.1.2 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 11.11.11.1/24	Configure interface IP address
Switch(config-if)# arp timeout 1200	Set ageing time
Switch(config-if)# arp retry-interval 2	Set request retry interval
Switch(config)# arp 11.11.11.2 1a.a011.eca2	Add static ARP entries

7.1.3 Command Validation

Validate ARP entries

Switch# show ip arp

```
Protocol  Address        Age (min)  Hardware Addr   Interface
Internet  11.11.11.2           -   001a.a011.eca2  eth-0-1
```

Switch# show ip arp summary

```
1 IP ARP entries, with 0 of them incomplete
(Static:0,  Dyamic:0, Interface:1)
ARP Pkt Received is: 0
ARP Pkt Send number is: 0
ARP Pkt Dicard number is: 0
```

Validate ARP request retry interval and aging time

Switch# show interface eth-0-1

```
Interface eth-0-1
  Interface current state: Administratively DOWN
  Hardware is Ethernet, address is 6c02.530c.2300 (bia 6c02.530c.2300)
  Bandwidth 1000000 kbits
  Index 1 , Metric 1 , Encapsulation ARPA
  Speed - Auto , Duplex - Auto  , Media type is 1000BASE_T
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  VRRP master of :  VRRP is not configured on this interface
  ARP timeout 12:20:00 AM,  ARP retry interval 2s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

7.2 ARP Proxy Configuration

7.2.1 Introduction

Proxy ARP is a variant of ARP protocol. If a computer without configured default gateway wants to communicate with other computers in the network, the gateway will respond to the source computer with its MAC address and destination computer IP address after receiving the ARP request from the source computer. Proxy ARP is to act as a host to respond to the ARP from another host. It enables to add a new router without prejudice to the routing table, to make the subnet more transparent to the host. Meanwhile, it also will bring about huge risks, including ARP cheating, ARP increase in a network segment, and even failure of network generalization of network topology. Proxy ARP has a main advantage of the ability of adding a new router on the network without prejudice to the routing table of other routers to make the changes of the subnet transparent to the host. Proxy ARP is usually applied in the network without a configured default gateway and routing policy.

Proxy ARP is classified into general ARP proxy and local ARP proxy.

Hosts linked to different device VLAN interfaces in a network segment can communicate with each other by means of layer 3 forwarding with the proxy ARP feature of the device.

To realize layer 3 intercommunication, if layer 2 port-isolate feature is enabled on the Ethernet switch or the switches under it, it is needed to enable the local proxy ARP feature. Note: Enabling local ARP proxy will automatically turn off ICMP redirecting.

7.2.2 Configure General ARP Proxy

I. Topology

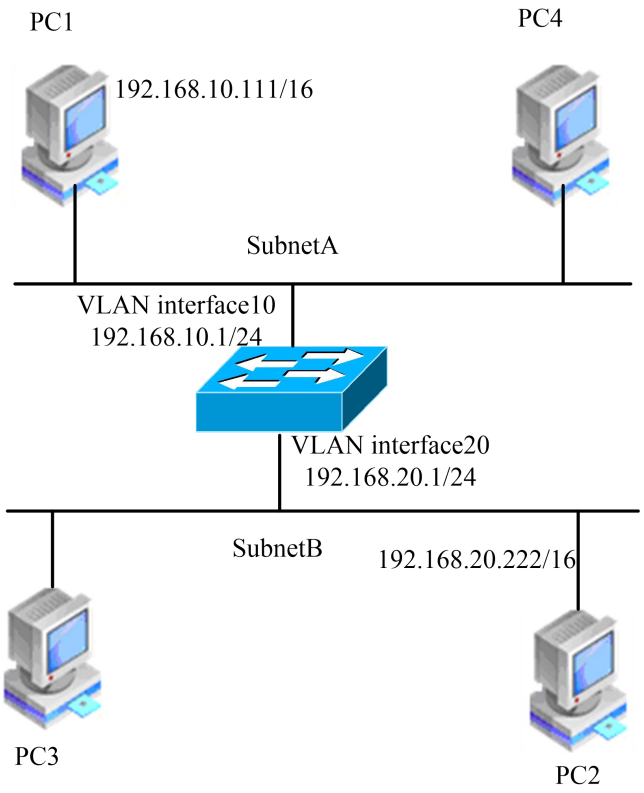


Figure 7-1 ARP Proxy Topology

II. Configuration

As shown in the figure above, PC1 belongs to VLAN10 and PC2 to VLAN20, and VLAN interface 10 and VLAN interface 20 are configured with ARP proxy respectively to realize intercommunication between PC1 and PC2.

The steps of enabling ARP proxy on VLAN10 and VLAN20 are as below.

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Enter VLAN database
Switch(config-vlan)# vlan 10,20	Create VLAN 10, VLAN 20
Switch(config-vlan)# exit	Exit VLAN database
Switch(config)# interface eth-0-22	Enter interface mode
Switch(config-if)# switchport access vlan 10	Add the interface into vlan 10
Switch(config-if)# no shutdown	Enable the interface

Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-23	Enter interface mode
Switch(config-if)# switchport access vlan 20	Add the interface into vlan 20
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface vlan 10	Create layer 3 interface 10, and enter interface mode
Switch(config-if)# ip address 192.168.10.1/24	Configure interface address
Switch(config-if)# proxy-arp enable	Enable ARP proxy
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface vlan 20	Create layer 3 interface 20, and enter interface mode
Switch(config-if)# ip address 192.168.20.1/24	Configure interface address
Switch(config-if)# proxy-arp enable	Enable ARP proxy
Switch(config-if)# exit	Exit interface mode

III. Command validation

Output Results on A Switch

Switch# show ip interface vlan 10

```
Interface vlan10
  Interface current state: UP
  Internet address(es):
    192.168.10.1/24 broadcast 192.168.10.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 1:00:00 AM,  ARP retry interval 1s
  ARP Proxy is enabled, Local ARP Proxy is disabled
  VRRP master of :  VRRP is not configured on this interface
```

Switch# show ip interface vlan 20

```
Interface vlan20
```

```
Interface current state: UP
Internet address(es):
  192.168.20.1/24 broadcast 192.168.20.255
Joined group address(es):
  224.0.0.1
The maximum transmit unit is 1500 bytes
ICMP error messages limited to one every 1000 milliseconds
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are always sent
ARP timeout 1:00:00 AM,  ARP retry interval 1s
ARP Proxy is enabled, Local ARP Proxy is disabled
VRRP master of :  VRRP is not configured on this interface
```

Switch# show ip arp

```
Protocol    Address         Age (min)  Hardware Addr   Interface
Internet    192.168.10.1          -   7cc3.11f1.aa00  vlan10
Internet    192.168.10.111        5   0cf9.11b6.6e2e  vlan10
Internet    192.168.20.1          -   7cc3.11f1.aa00  vlan20
Internet    192.168.20.222        6   5a94.031f.2357  vlan20
```

Output Results on PC1

[Host:~]$ ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 0C:F9:11:B6:6E:2E
          inet addr:192.168.10.111  Bcast:192.168.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:588 (588.0 b)  TX bytes:700 (700.0 b)
          Interrupt:5
```

[Host:~]$ arp –a

```
? (192.168.20.222) at 7c:c3:11:f1:aa:00 [ether] on eth0
```

[Host: ~]$ route -v

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.0.0     U     0      0        0 eth0
```

[Host:~]$ ping 192.168.20.222

```
PING 192.168.20.222 (192.168.20.222) 56(84) bytes of data.
64 bytes from 192.168.20.222: icmp_seq=0 ttl=63 time=189 ms
64 bytes from 192.168.20.222: icmp_seq=1 ttl=63 time=65.2 ms
--- 192.168.20.222 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 65.209/127.226/189.244/62.018 ms, pipe 2
```

Output Results on PC2

[Host:~]$ ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 5A:94:03:1F:23:57
          inet addr:192.168.20.222  Bcast:192.168.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:784 (784.0 b)  TX bytes:1174 (1.1 KiB)
          Interrupt:5
```

[Host:~]$ arp -a

```
? (192.168.10.111) at 7c:c3:11:f1:aa:00 [ether] on eth0
```

```
[Host: ~]$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.0.0     U     0      0        0 eth0
```

[Host: ~]$ ping 192.168.10.111

```
PING 192.168.10.111 (192.168.10.111) 56(84) bytes of data.
64 bytes from 192.168.10.111: icmp_seq=0 ttl=63 time=53.8 ms
64 bytes from 192.168.10.111: icmp_seq=1 ttl=63 time=65.8 ms
--- 192.168.10.111 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 53.832/59.842/65.852/6.010 ms, pipe 2
```

7.2.3 Configure Local Proxy ARP

I. Topology

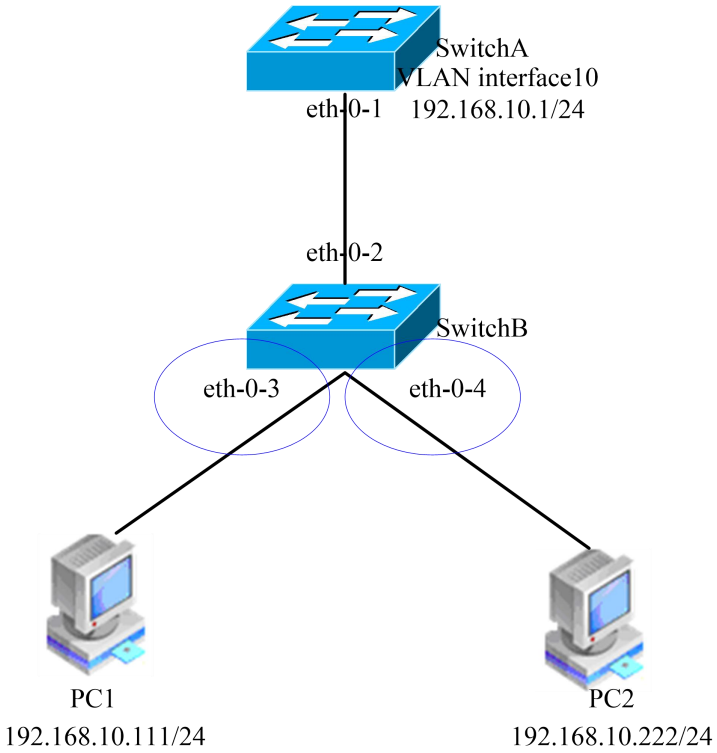


Figure 7-2 Local Proxy ARP Topology

II. Configuration

As shown in Figure 7-2, the three layer 2 interfaces eth2, eth3 and eth4 of Switch B all belong to VLAN10. Interfaces 3 and 4 both are in isolate group1, so they cannot intercommunicate with each other. Port 2 is in isolate group 3, so it can intercommunicate with Ports 3 and 4. PC1 and PC2 are connected to eth3 and eth 4 of Switch B respectively, both of which belong to VLAN10.

Layer 3 intercommunication can be realized between PCI and PC2 by the following steps:

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN database
Switch(config-vlan)# vlan 10	Create VLAN 10
Switch(config-vlan)# exit	Exit VLAN database
Switch(config)# interface eth-0-3	Enter interface mode
Switch(config-if)# switchport access vlan 10	Add the interface into vlan 10

Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-4	Enter interface mode
Switch(config-if)# switchport access vlan 10	Add the interface into vlan 10
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# switchport access vlan 10	Add the interface into vlan 10
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# port-isolate mode l2	Set port-isolate mode
Switch(config-if)# interface eth-0-3	Enter interface mode
Switch(config-if)# port-isolate group 1	Set the interface to belong to port-isolate group 1
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-4	Enter interface mode
Switch(config-if)# port-isolate group 1	Set the interface to belong to port-isolate group 1
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# port-isolate group 3	Set the interface to belong to port-isolate group 3
Switch(config-if)# exit	Exit interface mode

SwitchA

Switch# configure terminal	Enter configuration mode
Switch(config)# vlan database	Enter VLAN database
Switch(config-vlan)# vlan 10	Create VLAN 10
Switch(config-vlan)# exit	Exit VLAN database
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# switchport access vlan 10	Add the interface into vlan 10

Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface vlan 10	Create layer 3 interface vlan10, and enter interface mode
Switch(config-if)# ip address 192.168.10.1/24	Configure layer 3 address of the interface
Switch(config-if)# local-proxy-arp enable	Enable local proxy ARP
Switch(config-if)# exit	Exit interface mode

III.Command validation

Output Results on SwitchA

Switch# show ip arp

```
Protocol  Address         Age (min)  Hardware Addr   Interface
Internet  192.168.10.1          -   eeb4.2a8d.6c00  vlan10
Internet  192.168.10.111        0   34b0.b279.5f67  vlan10
Internet  192.168.10.222        0   2a65.9618.57fa  vlan10
```

Switch# show ip interface vlan 10

```
Interface vlan10
 Interface current state: UP
 Internet address(es):
  192.168.10.1/24 broadcast 192.168.10.255
 Joined group address(es):
  224.0.0.1
 The maximum transmit unit is 1500 bytes
 ICMP error messages limited to one every 1000 milliseconds
 ICMP redirects are never sent
 ICMP unreachables are always sent
 ICMP mask replies are always sent
 ARP timeout 1:00:00 AM,  ARP retry interval 1s
 ARP Proxy is disabled, Local ARP Proxy is enabled
 VRRP master of :  VRRP is not configured on this interface
```

Output Results on PC1

[Host: ~]$ ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 34:B0:B2:79:5F:67
          inet addr:192.168.10.111  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1344 (1.3 KiB)  TX bytes:2240 (2.1 KiB)
```

```
        Interrupt:5
```

[Host: ~]$ arp -a

```
? (192.168.10.222) at ee:b4:2a:8d:6c:00 [ether] on eth0
```

[Host: ~]$ ping 192.168.10.222

```
PING 192.168.10.222 (192.168.10.222) 56(84) bytes of data.
64 bytes from 192.168.10.222: icmp_seq=0 ttl=63 time=131 ms
64 bytes from 192.168.10.222: icmp_seq=1 ttl=63 time=159 ms
--- 192.168.10.222 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 131.078/145.266/159.454/14.188 ms, pipe 2
```

Output Results on PC2

[Host:~]$ ifconfig eth0

```
eth0      Link encap:Ethernet  HWaddr 2A:65:96:18:57:FA
          inet addr:192.168.10.222  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1600  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1148 (1.1 KiB)  TX bytes:1524 (1.4 KiB)
          Interrupt:5
```

[Host:~]$ arp -a

```
? (192.168.10.111) at ee:b4:2a:8d:6c:00 [ether] on eth0
```

[Host: ~]$ ping 192.168.10.111

```
PING 192.168.10.111 (192.168.10.111) 56(84) bytes of data.
64 bytes from 192.168.10.111: icmp_seq=0 ttl=63 time=198 ms
64 bytes from 192.168.10.111: icmp_seq=1 ttl=63 time=140 ms
64 bytes from 192.168.10.111: icmp_seq=2 ttl=63 time=146 ms
--- 192.168.10.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 140.196/161.959/198.912/26.267 ms, pipe 2
```

7.3 DHCP Client Configuration

7.3.1 Introduction

DHCP (Dynamic host configuration protocol) client dynamically obtains IP addresses and configuration parameters from DHCP server via DHCP protocol. If the client and server are in a same subnet, DHCP protocol interaction can be directly made between the client and server, otherwise a DHCP relay agent is needed to forward DHCP messages.

DHCP client requests IP addresses from DHCP server via DHCP broadcast message, and configures addresses and set the rent period after acquiring IP addresses and corresponding rent period. Starts sending DHCP messages to request continued use of the current IP addresses and

expect a new rent period upon entering the second half rent period. Once the rent is renewed, DHCP client updates the rent period.

The available options from DHCP client requesting from the server include: router, static-route, classless-static-route, classless-static-route-ms, tftp-server-address, dns-nameserver, domain-name, netbios-nameserver and vendor-specific. The followings are automatically requested by default: router, static-route, classless-static-route, classless-static-route-ms and tftp-server-address, which can be canceled via commands.

7.3.2 Configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no dhcp client request static-route	Cancel static-route request
Switch(config-if)# ip address dhcp	Enable DHCP client
Switch(config-if)# end	Exit to privilege mode

7.3.3 Command Validation

Check Interface Configuration

Switch# show running-config interface eth-0-1

```
Building configuration...
!
interface eth-0-1
 no switchport
 ip address dhcp
 no dhcp client request static-route
!
```

Check Working State of DHCP Client

Switch# show dhcp client verbose

```
DHCP client informations:
=========================================================
eth-0-1 DHCP client information:
  Current state: BOUND
  Allocated IP: 4.4.4.199 255.255.255.0
  Lease/renewal/rebinding: 1187/517/1037 seconds
  Lease from 2011-11-18 05:59:59 to 2011-11-18 06:19:59
  Will Renewal in 0 days 0 hours 8 minutes 37 seconds
```

```
DHCP server: 4.4.4.1
Transaction ID: 0x68857f54
Client ID: switch-7e39.3457.b700-eth-0-1
```

Show DHCP Client Statistics

Switch# show dhcp client statistics

```
DHCP client packet statistics:
=======================================================
DHCP OFFERS     received: 1
DHCP ACKs       received: 2
DHCP NAKs       received: 0
DHCP Others     received: 0
DHCP DISCOVER   sent: 1
DHCP DECLINE    sent: 0
DHCP RELEASE    sent: 0
DHCP REQUEST    sent: 2
DHCP packet send failed  : 0
```

7.4 DHCP Relay Configuration

7.4.1 Introduction

If the DHCP server and clients are in a same subnet, DHCP protocol interaction can be directly realized between the clients and server, without enabling DHCP Relay. If the DHCP server and clients are not in a same subnet, it is needed to enable DHCP Relay to forward DHCP messages to the external DHCP server.

DHCP Relay forwarding differs from normal IP routing transfer. The IP data packets forwarded via IP routing transfer are exchanged between networks transparently, while proxy DHCP Relay will generate a new DHCP message and send it to another interface while receiving a DHCP message. DHCP Relay agent sets gateway address and adds relay agent information (option82) in messages, and sends it to the DHCP server end. With DHCP relay agent, messages will be forwarded to clients after removal of option82 content once a response from the server is received.

7.4.2 Topological Graph

The figure below shows the network topology of testing DHCP Relay agent, where two PCs and one switch are needed to construct the testing environment.

- Computer A acts as DHCP server
- Computer B acts as DHCP client
- Switch acts as DHCP Relay agent

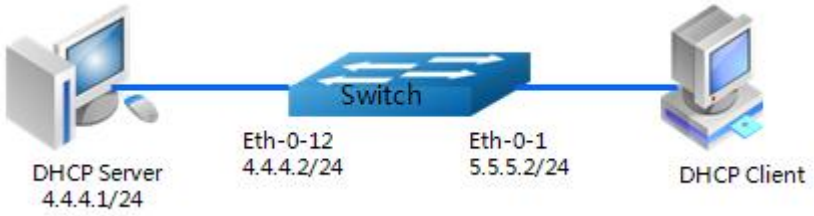


Figure 7-3 DHCP Relay Topological Graph

7.4.3 Configuration

Configure Interface eth-0-12

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-12	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# ip address 4.4.4.2/24	Set IP address
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface configuration mode

Configure DHCP Server Group

Switch(config)# dhcp-server 1 4.4.4.1	Create DHCP server group

Configure Interface eth-0-1

Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface.
Switch(config-if)# ip address 5.5.5.2/24	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# dhcp relay information trusted	Enable DHCP Relay option82 on the interface
Switch(config-if)# dhcp-server 1	Configure DHCP server
Switch(config-if)# exit	Exit interface configuration mode

Enable Global DHCP Relay Server

Switch(config)# service dhcp enable	Enable DHCP server
Switch(config)# dhcp relay	Enable DHCP Relay

7.4.4 Command Validation

Step 1 Check interface configuration.

Switch# show running-config interface eth-0-12

```
!
interface eth-0-12
 no switchport
 ip address 4.4.4.2/24
!
Switch# show running-config interface eth-0-1
!
interface eth-0-1
 no switchport
 dhcp relay information trusted
 dhcp-server 1
 ip address 5.5.5.2/24
!
```

Step 2 Check DHCP server status.

Switch# show services

```
Networking services configuration:
Service Name        Status
============================================================
dhcp                enable
```

Step 3 Check DHCP server group configuration.

Switch# show dhcp-server

```
DHCP server group information:
============================================================
group 1 ip address list:
[1] 4.4.4.1
```

Step 4 Show DHCP Relay statistics.

Switch# show dhcp relay statistics

```
DHCP relay packet statistics:
============================================================
Client relayed packets:  20
Server relayed packets:  20
```

```
Client error packets:    20
Server error packets:    0
Bogus GIADDR drops:      0
Bad circuit ID packets:  0
Corrupted agent options: 0
Missing agent options:   0
Missing circuit IDs:     0
```

Step 5 Check IP address obtained by the computer from DHCP server.

Ipconfig /all

```
Dhcp Enabled. . . . . . . . . .       . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . .         . : 5.5.5.1
Subnet Mask . . . . . .         . . . . : 255.255.255.0
Default Gateway . . . . . .     . . . : 5.5.5.2
DHCP Server . . . . . .         . . : 4.4.4.1
DNS Servers . . . . . .         . . . . : 4.4.4.1
```

7.5 DHCP Server Configuration

7.5.1 Introduction

DHCP server provides client with IP addresses and network configuration parameters via DHCP protocol. To render DHCP services, DHCP server must complete some basic configurations, such as distribution of address pool, setup of default gateway, and setup of network parameters. In real work, DHCP server will find available addresses from the set address pool to distribute to the requesting DHCP client, and send the requested network configuration parameters to the client. The distributed addresses and parameters are subject to a valid period (rent period), and clients are required to send a renewal request to the server before expiration so as to keep their IP addresses and renew the lease.

In practical condition, if DHCP server and DHCP client are in a same subnet, DHCP server can run normally after being directly connected to. Otherwise, DHCP server needs the aid of DHCP Relay in forwarding DHCP messages to render DHCP services to clients.

DHCP server supports the following options: bootfile-name, dns-server, domain-name, gateway, netbios-name-server, netbios-node-type and tftp-server-address. Additionally, it also supports some raw options.

7.5.2 Topology

Figure 5- 1: DHCP Server Topological Graph

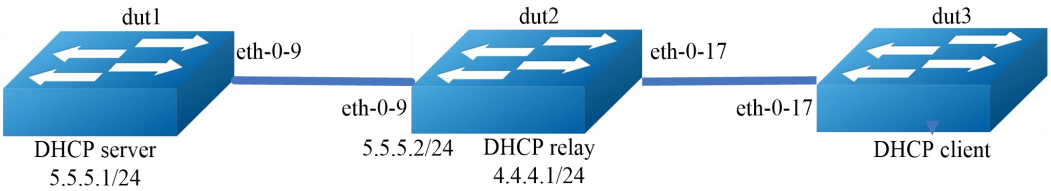


Figure 5-2: Topological Graph for DHCP Relay Participation

The figures above show the network topology for DHCP server testing.

7.5.3 Configuration

Topology1:

Configure DHCP Server (dut1)

Switch#configure terminal	Enter global configuration mode
Switch(config)# service dhcp enable	Globally enable DHCP service
Switch(config)#dhcp server	Globally enable DHCP server
Switch(config)#dhcp pool pool5	Add dhcp pool, and enter DHCP configuration mode
Switch(dhcp-config)#network 5.5.5.0/24	Configure address pool
Switch(dhcp-config)#gateway 5.5.5.1	Configure option: default gateway
Switch(dhcp-config)#exit	Exit DHCP configuration mode
Switch(config)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address 5.5.5.1/24	Configure IP address
Switch (config-if)# dhcp server enable	Enable DHCP server
Switch(config-if)# exit	Exit interface configuration mode

Configure DHCP Client (dut2)

Switch#configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address dhcp	Enable DHCP client
Switch(config-if)# exit	Exit interface configuration mode

Topology2:

Configure DHCP Server (dut1)

Switch#configure terminal	Enter global configuration mode
Switch(config)#service dhcp enable	Globally enable DHCP service
Switch(config)#dhcp server	Globally enable DHCP server
Switch(dhcp-config)#dhcp pool pool4	Add dhcp pool, and enter DHCP configuration mode
Switch(dhcp-config)#network 4.4.4.0/24	Configure address pool
Switch(dhcp-config)#gateway 4.4.4.1	Configure option: default gateway
Switch(dhcp-config)#exit	Exit DHCP configuration mode
Switch(config)# ip route 4.4.4.0/24 5.5.5.2	Add route
Switch(config)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address 5.5.5.1/24	Configure IP address
Switch (config-if)# dhcp server enable	Enable DHCP server
Switch(config-if)# exit	Exit interface configuration mode

Configure DHCP Relay (dut2)

Switch#configure terminal	Enter global configuration mode
Switch(config)#service dhcp enable	Globally enable DHCP service
Switch(config)#dhcp relay	Globally enable DHCP relay
Switch(config)#dhcp-server 1 5.5.5.1	Add DHCP server group
Switch(config)# interface eth-0-17	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address 4.4.4.1/24	Configure IP address
Switch (config-if)# dhcp-server 1	Select DHCP server group
Switch(config-if)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address 5.5.5.2/24	Configure IP address

Switch(config-if)# exit	Exit interface configuration mode

Configure DHCP Client (dut3)

Switch#configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-17	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# ip address dhcp	Enable DHCP client
Switch(config-if)# exit	Exit interface configuration mode

7.5.4 Command Validation

Topology1:

View DHCP Server (dut1) Configuration:

Switch# show running-config

```
!
service dhcp enable
!
interface eth-0-9
 no switchport
 dhcp server enable
 ip address 5.5.5.1/24!
!
dhcp server
dhcp pool pool5
 network 5.5.5.0/24
 gateway 5.5.5.1
```

View DHCP client state on DHCP Server (dut1):

Switch# show dhcp client verbose

```
DHCP client informations:
=========================================================
eth-0-9 DHCP client information:
  Current state: BOUND
  Allocated IP: 5.5.5.2 255.255.255.0
  Lease/renewal/rebinding: 1194/546/1044 seconds
  Lease from 2/4/2012 7:40:12 AM to 2/4/2012 8:00:12 AM
  Will Renewal in 0 days 0 hours 9 minutes 6 seconds
  DHCP server: 5.5.5.1
  Transaction ID: 0x45b0b27b
  Default router: 5.5.5.1
```

```
  Classless static route:
    Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 5.5.5.1
  TFTP server addresses: 5.5.5.3
Client ID: switch-6e6e.361f.8400-eth-0-9
```

View DHCP server statistics on DHCP Server (dut1):

Switch# show dhcp server statistics

```
DHCP server packet statistics:
=======================================================
Message Received:
BOOTREQUEST:  0
DHCPDISCOVER:  1
DHCPREQUEST:  1
DHCPDECLINE:  0
DHCPRELEASE:  0
DHCPINFORM:  0
Message Sent:
BOOTREPLY:  0
DHCPOFFER:  1
DHCPACK:  1
DHCPNAK:  0
```

View DHCP server address assignment and interface information on DHCP Server (dut1):

Switch# show dhcp server binding all

```
IP address      Client-ID/          Lease expiration          Type
                Hardware address
5.5.5.2         6e:6e:36:1f:84:00   Sat 2012.02.04 08:00:12   Dynamic
```

Switch# show dhcp server interfaces

```
List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
=======================================================
eth-0-9
```

Topology2:

View DHCP Server (dut1) Configuration:

Switch# show running-config

```
!
service dhcp enable
!
interface eth-0-9
 no switchport
 dhcp server enable
 ip address 5.5.5.1/24!
!
ip route 4.4.4.0/24 5.5.5.2
!
dhcp server
```

```
dhcp pool pool4
 network 4.4.4.0/24
 gateway 4.4.4.1
```

View DHCP client state on DHCP Server (dut1):

Switch# show dhcp client verbose

```
DHCP client informations:
=========================================================
eth-0-17 DHCP client information:
  Current state: BOUND
  Allocated IP: 4.4.4.5 255.255.255.0
  Lease/renewal/rebinding: 1199/517/1049 seconds
  Lease from 2/6/2012 5:23:09 AM to 2/6/2012 5:43:09 AM
  Will Renewal in 0 days 0 hours 8 minutes 37 seconds
  DHCP server: 5.5.5.1
  Transaction ID: 0x192a4f7d
  Default router: 4.4.4.1
  Classless static route:
    Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 4.4.4.1
  TFTP server addresses: 5.5.5.3
  Client ID: switch-3c9a.b29a.ba00-eth-0-17
```

View DHCP server statistics on DHCP Server (dut1):

Switch# show dhcp server statistics

```
DHCP server packet statistics:
=========================================================
Message Received:
BOOTREQUEST:  0
DHCPDISCOVER:  1
DHCPREQUEST:  1
DHCPDECLINE:  0
DHCPRELEASE:  0
DHCPINFORM:  0
Message Sent:
BOOTREPLY:  0
DHCPOFFER:  1
DHCPACK:  1
DHCPNAK:  0
```

View DHCP server address assignment and interface information on DHCP Server (dut1):

Switch# show dhcp server binding all

```
IP address      Client-ID/          Lease expiration          Type
                Hardware address
 4.4.4.5        3c:9a:b2:9a:ba:00   Mon 2012.02.06 05:43:09   Dynamic
```

Switch# show dhcp server interfaces

```
List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
```

==========

eth-0-9

7.6 DNS Configuration

7.6.1 Introduction

DNS is short for domain name system. It is a distributed database that enables you to map a hostname to an IP address. You can use a hostname to replace an IP address in all IP-related commands (such as ping, telent, connect) and other telnet-supporting actions when configuring DNS on switches.

IP is defined as a stratified name abstract. The domain names are separated with dot mark.

To resolve domain names, a domain name server must be defined, in which domain name cache (or database) of IP addresses resolved from domain names is saved. To resolve a domain name into an IP address, users must assign a valid server of the network, and then enable DNS.

7.6.2 Topology

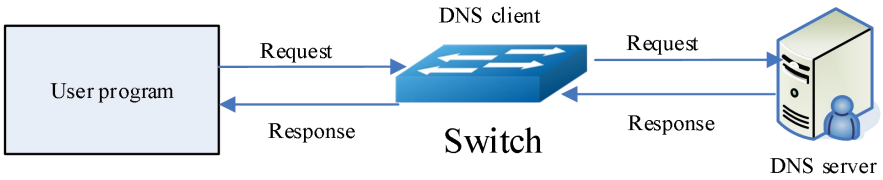


Figure 7-4 Typical DNS Topology

7.6.3 Configuration

Switch#configure terminal	Enter global configuration mode
Switch(config)#dns domain server1	Name a default domain name system for mapping host domain names (non-dotted decimal string) to IP addresses.
Switch(config)#dns server 202.100.10.20	Configure Ipv4 address for the domain name server in the DNS (DNS is used for internal domain name query).
Switch(config)# ip host www.example1.com 192.0.2.141	Set hostname in a static domain name resolution table and corresponding host IPv4 address

Command validation

Switch# show dns server

```
Current DNS name server configuration:
    Server              IP Address
-----------------------------------------------------------------
1   nameserver          202.100.10.20
```

8 IP Routing Configuration Guide

8.1 IP Unicast-Routing Configuration

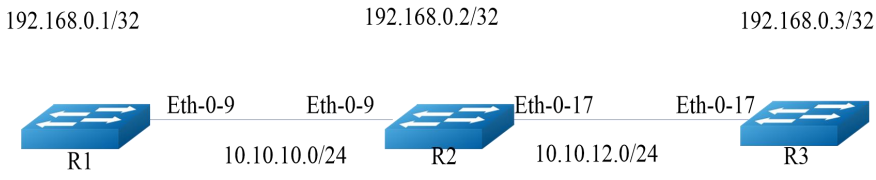
8.1.1 Introduction

Static routing is a special route that is manually configured by administrators In the case of simple network structure, configuring a static route is enough for normal operation of network. Rationally setting and using a static route helps improving network performance and guaranteeing bandwidth for important network applications. Static route has a defect as follows: in the case of network malfunction or topological changes, the route might become unreachable, to result in network interruption. In such case, network administer manually changing the static routing configuration is required.

This example demonstrates how to enable a static route in a simple network topological structure. Static routing is of great use in small networks. Static routing can provide a simple solution to make several destinations reachable. For large networks, dynamic routing protocol applies. A static route consists of a network prefix (host address) and a next hop (gateway).

Router R1 is configured with three static routes, including a remote network 10.10.12.0/24 and two loopback addresses (host address) to Routers R2 and R3 respectively. Router R3 is configured with a default static route, equal to that a same gateway or next hop address is used for configuration of individual static routs. Router R2 has two routes, and the destination of each route is the loopback interface address of the remote router.

8.1.2 Topology



8.1.3 Configuration

R1

Switch# configure terminal	Enter global configuration mode

Switch(config)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface UP
Switch(config-if)# no switchport	Set as layer3 interface
Switch(config-if)# ip address 10.10.10.1/24	Configure IP address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface loopback 0	Assign loopback interface to be configured
Switch(config-if)# ip address 192.168.0.1/32	Configure IP address and 32bit mask as host address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# ip route 10.10.12.0/24 10.10.10.2 Switch(config)# ip route 192.168.0.2/32 10.10.10.2 Switch(config)# ip route 192.168.0.3/32 10.10.10.2	Assign the network needed by the destination prefix and mask gateway, such as 10.10.12.0/24, and add gateway for each one(10.10.10.2 in all cases). Since R2 is the only available next hop, it can be configured as a default route rather than an individual address, see R3 configuration

R2

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-9	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# no switchport	Set as layer3 interface
Switch(config-if)# ip address 10.10.10.2/24	Configure IP address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface eth-0-17	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# no switchport	Set as layer3 interface
Switch(config-if)# ip address 10.10.12.2/24	Set IP address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface loopback 0	Assign loopback interface to be configured
Switch(config-if)# ip address 192.168.0.2/32	Configure IP address and 32bit mask as host address
Switch(config-if)# exit	Exit interface configuration mode

Switch(config)# ip route 192.168.0.1/32 10.10.10.1 Switch(config)# ip route 192.168.0.3/32 10.10.12.3	Assign destination and mask, and add gateway

R3

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-17	Enter interface configuration mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# no switchport	Set as layer3 interface
Switch(config-if)# ip address 10.10.12.3/24	Set IP address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# interface loopback 0	Assign loopback interface to be configured
Switch(config-if)# ip add 192.168.0.3/32	Configure IP address and 32bit mask as host address
Switch(config-if)# exit	Exit interface configuration mode
Switch(config)# ip route 0.0.0.0/0 10.10.12.2	Assign 10.10.12.2 as the default gateway for reaching any network, because 10.10.12.2 is the only one route that can be assigned as a default gateway rather than a gateway of an individual network or host.

8.1.4 Command Validation

R 1

```
R1# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.10.0/24 is directly connected, eth-0-9
C      10.10.10.1/32 is in local loopback, eth-0-9
S      10.10.12.0/24 [1/0] via 10.10.10.2, eth-0-9
C      192.168.0.1/32 is directly connected, loopback0
S      192.168.0.2/32 [1/0] via 10.10.10.2, eth-0-9
S      192.168.0.3/32 [1/0] via 10.10.10.2, eth-0-9
```

R 2

```
R2# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.10.0/24 is directly connected, eth-0-9
C      10.10.10.2/32 is in local loopback, eth-0-9
C      10.10.12.0/24 is directly connected, eth-0-17
C      10.10.12.2/32 is in local loopback, eth-0-17S      192.168.0.1/32 [1/0] via 10.10.10.1, eth-0-9
C      192.168.0.2/32 is directly connected, loopback0
S      192.168.0.3/32 [1/0] via 10.10.12.3, eth-0-17
```

R 3

```
R3# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
Gateway of last resort is 10.10.12.2 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 10.10.12.2, eth-0-17
C      10.10.12.0/24 is directly connected, eth-0-17
C      10.10.12.3/32 is in local loopback, eth-0-17
C      192.168.0.3/32 is directly connected, loopback0
```

8.2 RIP Configuration

8.2.1 Introduction

RIPRouting information protocol (Routing information protocol) is a simple interior gateway protocol (IGP) that is mainly applied in small-scale networks.

RIP is a protocol based on distance-vector algorithm, which conducts routing information exchange via UDP message. RIP measures the distance from the destination via hop count, which is called routing cost. In RIP, the hop count of moving from a router to the directly connected network is 0, that of moving to the network reachable via one router is 1, and so on. To limit the convergence time, RIP specifies cost value to be an integer between 0 and 15, and a hop count with cost value above or equal to 16 is defined as infinity, meaning unreachability of destination network or host.

To enhance the performance and prevent routing loops, RIP supports split horizon. RIP also can introduce routes obtained based on other routing protocols.

8.2.2 Configure RIP Enabling

The steps of enabling RIP routing protocol on two switches are as shown in Figure 8-1.

I. Topology

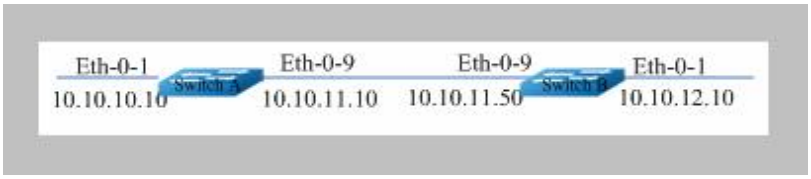


Figure 8-1 RIP Topology

II. Configuration

Switch A

SwitchA# configure terminal	Enter configuration mode
SwitchA(config)# interface eth-0-1	Enter interface mode
SwitchA(config-if)# no switchport	Set the interface as layer3 interface
SwitchA(config-if)# ip address 10.10.10.10/24	Configure IP address
SwitchA(config-if)# exit	Exit interface mode
SwitchA(config)# interface eth-0-9	Enter interface mode
SwitchA(config-if)# no switchport	Set the interface as layer3 interface
SwitchA(config-if)# ip address 10.10.11.10/24	Configure IP address
SwitchA(config-if)# exit	Exit interface mode
SwitchA(config)# router rip	Enable RIP routing protocol
SwitchA(config-router)#network 10.10.10.0/24	Distribute 10.10.10.0 network segment into RIP routing protocol
SwitchA(config-router)#network 10.10.11.0/24	Distribute 10.10.11.0 network segment into RIP routing protocol

Switch B

SwitchB# configure terminal	Enter configuration mode
SwitchB(config)# interface eth-0-1	Enter interface mode

SwitchB(config-if)# no switchport	Set the interface as layer3 interface
SwitchB(config-if)# ip address 10.10.12.10/24	Configure IP address
SwitchB(config-if)# exit	Exit interface mode
SwitchB(config)# interface eth-0-9	Enter interface mode
SwitchB(config-if)# no switchport	Set the interface as layer3 interface
SwitchB(config-if)# ip address 10.10.11.50/24	Set IP address
SwitchB(config)# router rip	Enable RIP routing protocol
SwitchB(config-router)#network 10.10.11.0/24	Distribute 10.10.11.0 network segment into RIP routing protocol
SwitchB(config-router)#network 10.10.12.0/24	Distribute 10.10.11.0 network segment into RIP routing protocol

III. Command validation

Use the following command to validate the configuration above:

show ip rip database，show ip protocols rip，show ip rip interface 和 show ip route

Switch A output

```
SwitchA# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
      C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network          Next Hop       Metric From          If      Time
Rc 10.10.10.0/24                     1                 eth-0-1
Rc 10.10.11.0/24                     1                 eth-0-9
R  10.10.12.0/24     10.10.11.50      2 10.10.11.50     eth-0-9  00:02:52
SwitchA# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 17 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send         Recv   Key-chain
    eth-0-1          2            2
    eth-0-9          2            2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.50           120  00:00:22              0           0
```

```
  Number of routes (including connected): 3
  Distance: (default is 120)
SwitchA# show ip rip interface
eth-0-1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
SwitchA# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.10.0/24 is directly connected, eth-0-1
C      10.10.10.10/32 is in local loopback, eth-0-1
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.10/32 is in local loopback, eth-0-9
R      10.10.12.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:25:50
```

8.2.3 Configure RIP Version

Configure the RIP version sending and receiving via routed ports. In the example below, the RIP versions sent and received by Switch B via eth-0-9 and eth-0-20 are v1 and v2 respectively.

I. Topology

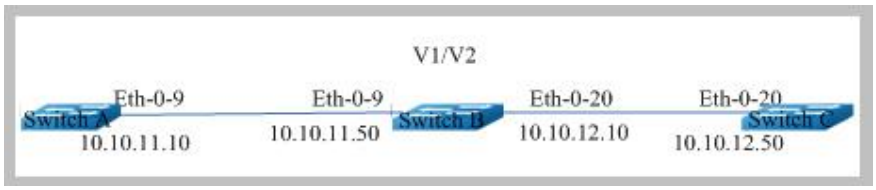


Figure 8-2 RIP Topology II

II. Configuration

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# router rip	Enable RIP routing protocol.
Switch(config-router)# exit	Exit router mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# ip rip send version 1 2	Configure the RIP version sending via the interface
Switch(config-if)# ip rip receive version 1 2	Configure the RIP version receiving via the interface
Switch (config-if)# quit	Exit interface mode
Switch(config)# interface eth-0-20	Enter interface mode
Switch(config-if)# ip rip send version 1 2	Configure the RIP version sending via the interface
Switch(config-if)# ip rip receive version 1 2	Configure the RIP version receiving via the interface

III. Command validation

Use the following command to validate the configuration above:

show ip rip database，Show running-config，show ip protocols rip，show ip rip interface 和 show ip route

Switch B output

```
Switch# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
    C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
  Network          Next Hop      Metric From        If     Time
R  10.0.0.0/8                      1              eth-0-9
Rc 10.10.11.0/24                    1              eth-0-9
```

```
Rc 10.10.12.0/24                    1               eth-0-20
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 1 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface       Send         Recv   Key-chain
    eth-0-9         1 2          1 2
    eth-0-20        1 2          1 2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway         Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.10          120  00:00:22              0           0
    10.10.12.50          120  12:00:27 AM           0           0
  Number of routes (including connected): 3
  Distance: (default is 120)
Switch# show ip rip inter
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
eth-0-20 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
Switch# show run
interface eth-0-9
 no switchport
 ip address 10.10.11.50/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth-0-20
 no switchport
 ip address 10.10.12.10/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
```

```
 network 10.10.11.0/24
 network 10.10.12.0/24
```

Switch A output

```
Switch# show running-config
interface eth-0-9
 no switchport
 ip address 10.10.11.10/24
!
router rip
 network 10.10.11.0/24
```

Switch C output

```
Switch# show running-config
interface eth-0-20
 no switchport
 ip address 10.10.12.50/24
!
router rip
 network 10.10.12.0/24
```

8.2.4 Configure Metric Parameters

Attached metric refers to input/output metric attached to RIP routing, including sending and receiving attached metric. Sending attached metric will not change the routing metric in the routing table, which will be added to the sending router only when the interface sends RIP routing information; receiving attached metric will affect the received routing metric, and the interface that receives a legal RIP route will attach the metric to the route while adding it to the routing table. Attached metric generally contains the following parameters:

- The ACL parameters for specifying adding routing metric are described as below.
  - **In**: applies to RIP routes learned from neighboring routers
  - **Out**: applies to the RIP announcement delivered to neighboring routers
- Offset value metric matching ACL routing
- Interface with offset-list applied

  If a route matches the global offset table (not assign an interface) and an interface-based offset table, the interface-based table is prior. In such case, the metric of the interface-based is added to the route.

The example below shows how to add metric 3 to 1.1.1.0 on eth-0-13 of Switch A.

I. Topology

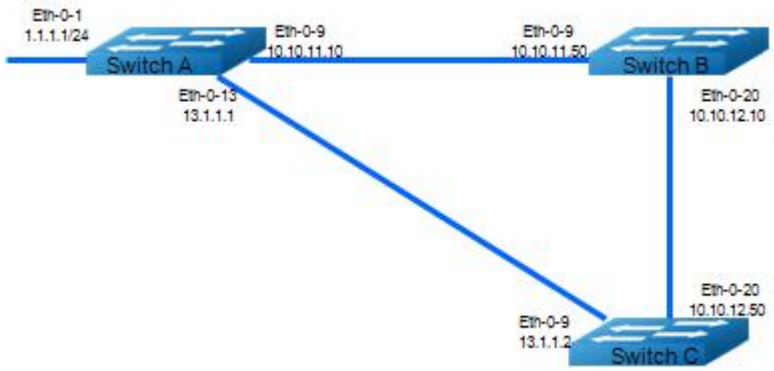


Figure 8-3 RIP Topology III

II. Configuration

Switch A configuration

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
interface eth-0-13
no switchport
ip address 13.1.1.1/24
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
network 13.1.1.0/24
```

Switch B configuration

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch C configuration

```
interface eth-0-13
no switchport
ip address 13.1.1.2/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router rip
network 10.10.12.0/24
network 13.1.1.0/24
```

Validation route table on Switch C

```
Switch# show ip route rip
R     1.1.1.0/24 [120/2] via 13.1.1.1, eth-0-13, 12:07:46 AM
R     10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 12:07:39 AM
            [120/2] via 10.10.12.10, eth-0-20, 00:07:39
Change router 1.1.1.0/24 via 10.10.12.10
```

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)#ip access-list ripoffset	Create ACL.
Switch(config-ip-acl)# permit any 1.1.1.0 0.0.0.255 any	Match corresponding network segment
Switch(config-ip-acl)# router rip	Enable RIP routing protocol
Switch(config-router)# offset-list ripoffset out 3 eth-0-13	Set the metric value for offset list

III. Command validation

Switch C output

Switch# show ip route rip

```
R     1.1.1.0/24 [120/3] via 10.10.12.10, eth-0-20, 12:00:02 AM
R     10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 12:11:40 AM
            [120/2] via 10.10.12.10, eth-0-20, 12:11:40 AM
```

8.2.5 Configure Administrative Distance

By default, the administrative distance of RIP is 120. In case of route comparison, the route with a short administrative distance stands a big chance of being selected.

The example below shows how to change RIP administrative distance.

I. Topology

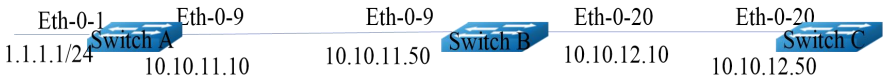


Figure 8-4 RIP Topology IV

II. Configuration

Switch A configuration

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router ospf
network 1.1.1.0/24 area 0
network 10.10.11.0/24 area 0
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
```

Switch B configuration

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router ospf
network 10.10.11.0/24 area 0
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch C configuration

```
interface eth-0-20
no switchport
```

```
ip address 10.10.12.50/24
!
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.12.0/24
```

Switch C output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
O      1.1.1.0/24 [110/3] via 10.10.12.10, eth-0-20, 01:05:49
O      10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 01:05:49
C      10.10.12.0/24 is directly connected, eth-0-20
C      10.10.12.50/32 is in local loopback, eth-0-20
```

The steps of changing RIP administrative distance of 1.1.1.0 segment on Switch C are as below.

Switch# configure terminal	Enter configuration mode
Switch(config)#ip access-list ripdistancelist	Create ACL
Switch(config-ip-acl)# permit any 1.1.1.0 0.0.0.255 any	Match corresponding network segment
Switch(config-ip-acl)# router rip	Enable RIP routing protocol
Switch(config-router)# distance 100 0.0.0.0/0 ripdistancelist	Set RIP route administrative distance as 100 0.0.0.0/0 is the prefix of the source IP, and the administrate distance of all routes matching the network segment will be set as 100

III. Command validation

Switch C output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
```

R 1.1.1.0/24 [100/3] via 10.10.12.10, eth-0-20, 12:00:02 AM
O 10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 1:10:42 AM
C 10.10.12.0/24 is directly connected, eth-0-20
C 10.10.12.50/32 is in local loopback, eth-0-20

8.2.6 Configure Redistribution

You can redistribute static routing, direct-connected routing and other routing protocols such as OSPF routing to RIP, which will be sent by RIP to its neighbors.

The default RIP redistribution metric is 1, and the maximum is 16.

For redistributing a specific route to RIP, the metric can be the default value or a modified value.

The example below shows how to redistribute other routing information to RIP.

I. Topology

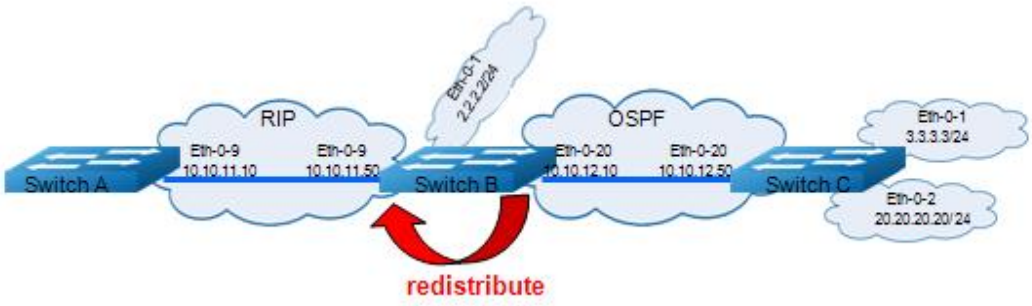


Figure 8-5 RIP Topology V

II. Configuration

Switch A configuration

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
```

Switch B configuration

```
interface eth-0-1
no switchport
ip address 2.2.2.2/24
!
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
```

```
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
!
ip route 20.20.20.0/24 10.10.12.50
```

Switch C configuration

```
interface eth-0-1
no switchport
ip address 3.3.3.3/24
!
interface eth-0-2
no switchport
ip address 20.20.20.20/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router ospf
network 3.3.3.0/24 area 0
network 10.10.12.0/24 area 0
```

Switch A output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.10/32 is in local loopback, eth-0-9
```

Switch B output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
```

```
C     2.2.2.0/24 is directly connected, eth-0-1
C     2.2.2.02/32 is in local loopback, eth-0-1
O     3.3.3.0/24 [110/2] via 10.10.12.50, eth-0-20, 1:05:41 AM
C     10.10.11.0/24 is directly connected, eth-0-9
C     10.10.11.50/32 is in local loopback, eth-0-9
C     10.10.12.0/24 is directly connected, eth-0-20
C     10.10.12.10/24 is in local loopback, eth-0-20
S     20.20.20.0/24 [1/0] via 10.10.12.50, eth-0-20
```

Switch B Configure Redistribute

Switch# configure terminal	Enter configuration mode
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)#default-metric 2	Specify default metric
Switch(config-router)# redistribute static	Redistribute static route
Switch(config-router)# redistribute connected	Redistribute direct-connected route
Switch(config-router)#redistribute ospf metric 5	Redistribute OSPF route to RIP
Switch(config)# router ospf	Enable OSPF routing protocol
Switch(config-router)# redistribute connected	Redistribute direct-connected route

III. Command validation

Switch A output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
        * - candidate default
R     2.2.2.0/24 [120/3] via 10.10.11.50, eth-0-9, 12:02:36 AM
R     3.3.3.0/24 [120/6] via 10.10.11.50, eth-0-9, 12:02:26 AM
C     10.10.11.0/24 is directly connected, eth-0-9
C     10.10.11.10/32 is in local loopback eth-0-9
R     10.10.12.0/24 [120/3] via 10.10.11.50, eth-0-9, 12:02:36 AM
R     20.20.20.0/24 [120/3] via 10.10.11.50, eth-0-9, 12:02:41 AM
```

8.2.7 Configure Split Horizon Parameters

In general, for routers connected a broadcast network and using distance vector routing protocol, split horizon mechanism is applied to prevent loops. By applying the split horizon mechanism, the routes learned from an interface cannot be released out via the interface, which generally optimizes the communication between multiple routers, especially in the case of link failure. By

configuring poison reverse, the routes learned from an interface can be released out via the interface, but they are unreachable because the metric value of the routes has been set as 16.

I. Topology

Figure 8-6 RIP Topology VI

II. Configuration

Switch A Configuration

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
redistribute connected
```

Switch B Configuration

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
router rip
network 10.10.11.0/24
```

Switch B debug Configuration

```
Switch# debug rip packet send detail
Switch# terminal monitor
```

Disable Split-horizon on Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-9	Configure interface eth-0-9
Switch(config-if)# no ip rip split-horizon	Disable split horizon

```
Apr  8 06:24:25 Switch RIP4-7: SEND[eth-0-9]: Send to 224.0.0.9:520
```

```
Apr  8 06:24:25 Switch RIP4-7: SEND[eth-0-9]: RESPONSE version 2 packet size 44
Apr  8 06:24:25 Switch RIP4-7: 1.1.1.0/24 -> 0.0.0.0 family 2 tag 0 metric 2
Apr  8 06:24:25 Switch RIP4-7: 10.10.11.0/24 -> 0.0.0.0 family 2 tag 0 metric 1
```

Enable Split-horizon on Switch B

Switch(config-if)# ip rip split-horizon	Enable split horizon
Switch(config-if)# ip rip split-horizon poisoned	Enable poison reverse

```
Apr  8 6:38:35 AM Switch RIP4-7: SEND[eth-0-9]: Send to 224.0.0.9:520
Apr  8 6:38:35 AM Switch RIP4-7: SEND[eth-0-9]: RESPONSE version 2 packet size 44
Apr  8 6:38:35 AM Switch RIP4-7: 1.1.1.0/24 -> 0.0.0.0 family 2 tag 0 metric 16
Apr  8 6:38:35 AM Switch RIP4-7: 10.10.11.0/24 -> 0.0.0.0 family 2 tag 0 metric 16
```

III. Command validation

Use the following command to validate the configuration above:

show running-config 和 show ip rip interface

8.2.8 Configure Timers

RIP is controlled by several timers, such as frequency of routing update, routing failure time, etc. You can adjust RIP performance by adjusting these timers, to address your needs in Internet works better. The following parameters can be adjusted:

- Update timer defines the interval of sending update messages.
- Timeout timer defines the routing aging time. If no route update message is received within the aging time, the metric value of the route in the routing table will be set as 16.
- Garbage-Collect timer defines the period from the route metric value being changed to 16 until the route is removed from the routing table.

I. Configuration

Use the following commands to configure Timer.

Switch# configure terminal	Enter configuration mode
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# timers basic 10 180 120	Specify routing table update timer as 10 seconds, routing information timeout timer as 180 seconds, and garbage collect timer as 120 seconds.

II. Command validation

Use the following command to validate the configuration above:

show running-config 和 show ip protocols rip

Switch# show ip protocols rip

```
Routing protocol is "rip"
  Sending updates every 10 seconds with +/-5 seconds, next due in 2 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send        Recv   Key-chain
    eth-0-9          2           2
  Routing for Networks:
    10.10.11.0/24
  Routing Information Sources:
    Gateway         Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.50          120  12:00:02 AM            0           0
  Number of routes (including connected): 5
  Distance: (default is 120)
```

8.2.9 Configure RIP Route Filter List

Routers provide the function of routing information filter, with which ingress or egress filtering policy can be configured by specifying an access control list and address prefix list to filter received or released routes. A route filter list generally contains the following parameters:

- An ACL or prefix list used as filter.
- **Ingress:** The filter is applied to the learned route; Routing information protocol The filter is applied to the releasing route.
- Interface for applying filter (optional).

I. Topology

Figure 8-7 RIP Topology VII

II. Configuration

Switch A configuration

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
```

```
router rip
network 10.10.11.0/24
```

Switch B configuration

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-2
no switchport
ip address 2.2.2.2/24
!
interface eth-0-3
no switchport
ip address 3.3.3.3/24
!
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
router rip
network 1.1.1.0/24
network 2.2.2.0/24
network 3.3.3.0/24
network 10.10.11.0/24
```

Switch A output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R      1.1.1.0/24 [120/2] via 10.10.11.50, eth-0-9, 12:01:50 AM
R      2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 12:01:50 AM
R      3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 12:01:50 AM
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.10/32 is in local loopback, eth-0-9
```

Please refer to the commands in the table below for configuring Switch B.

Switch# configure terminal	Enter configuration mode
Switch(config)# ip prefix-list 1 deny 1.1.1.0/24 Switch(config)# ip prefix-list 1 permit any	Establish a list
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# distribute-list prefix 1 out	Apply policy

III. Command validation

Switch A output

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R      2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 12:00:08 AM
R      3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 12:00:08 AM
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.10/32 is in local loopback, eth-0-9
```

8.2.10 Configure RIPv2 Authentication (single key)

RIP-2 supports two authentication methods: plaintext authentication and MD5 ciphertext authentication. This example shows how to implement plaintext authentication. Switch A and Switch B are running RIP routing protocol. The steps of configuring plaintext authentication of the switches are as below:

Step 1 Assign an interface, and define the interface password.

Step 2 Specify plaintext authentication as the authentication method.

Any RIP data packet received via the assigned interface should be set with a same string as password. Similarly, Switch B also requires the same password and authentication method.

I. Topology

Figure 8-8 RIPv2

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Configure interface eth-0-1
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address
Switch(config-if)# exit	Exit interface mode

Switch(config-if)# interface eth-0-9	Configure interface eth-0-9
Switch(config-if)# ip address 10.10.11.10/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# network 10.10.11.0/24	Release the network segment into RIP routing
Switch(config-router)# redistribute connected	Redistribute direct-connected route
Switch(config-router)# exit	Exit router mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# ip rip authentication string Auth1	Specify authentication string
Switch(config-if)# ip rip authentication mode text	Specify authentication mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Configure interface eth-0-1
Switch(config-if)# ip address 2.2.2.2/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config-if)# interface eth-0-9	Configure interface eth-0-9
Switch(config-if)# ip address 10.10.11.50/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# network 10.10.11.0/24	Release the network segment into RIP routing
Switch(config-router)# redistribute connected	Redistribute direct-connected route
Switch(config-router)# exit	Exit router mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# ip rip authentication string Auth1	Specify authentication string
Switch(config-if)# ip rip authentication mode text	Specify authentication mode

III. Command validation

Use the following commands to validate the configuration above:

show running-config, show ip rip database, show ip protocols rip, show ip rip interface and show ip route

8.2.11 Configure RIPv2 MD5 Authentication (multiple keys)

This example shows how to implement MD5 authentication for the process of RIP routing information exchange. For Switch A and Switch B needing MD5 authentication, define a key chain first, then specify keys and configure authentication string or password, and define the effective time of the keys by specifying the receiving or sending time. Apply the key chain to an interface, and specify MD5 as the authentication mode of the interface. The key configurations of Switch A and of Switch B must be the same to make sure successful RIP routing update information exchange. For MD5 authentication, both key ID and key string must be matched. In the example below, we also configure the effective time of key, so that key update happens every 5 days.

I. Topology

Figure 8-9 RIPv2 MD5 authentication

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Configure interface eth-0-1
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config-if)# interface eth-0-9	Configure interface eth-0-9
Switch(config-if)# ip address 10.10.11.10/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# network 10.10.11.0/24	Release the network segment into RIP routing
Switch(config-router)# redistribute connected	Redistribute direct-connected route

Switch(config-router)# exit	Exit router mode
Switch(config)# key chain SUN	Define key chain
Switch(config-keychain)# key 1	Create key id 1
Switch(config-keychain-key)# key-string key1	Set password
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2012 14:00:00 Mar 7 2012	Set accept lifetime
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2012 12:00:00 Mar 7 2012	Set send lifetime
Switch(config-keychain-key)# exit	Exit
Switch(config-keychain)# key 2	Create key id 2
Switch(config-keychain-key)# key-string Earth	Set password
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2012 14:00:00 Mar 12 2012	Set accept lifetime
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 7 2012 12:00:00 Mar 12 2012	Set send lifetime
Switch(config-keychain-key)# end	Exit
Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# ip rip authentication key-chain SUN	Define interface authentication name
Switch(config-if)# ip rip authentication mode md5	Define interface authentication mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Configure interface eth-0-1
Switch(config-if)# ip address 2.2.2.2/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config-if)# interface eth-0-9	Configure interface eth-0-9
Switch(config-if)# ip address 10.10.11.50/24	Configure IP address
Switch(config-if)# exit	Exit interface mode

Switch(config)# router rip	Enable RIP routing protocol
Switch(config-router)# network 10.10.11.0/24	Release the network segment into RIP routing
Switch(config-router)# redistribute connected	Redistribute direct-connected route
Switch(config-router)# exit	Exit router mode
Switch(config)# key chain SUN	Define key chain
Switch(config-keychain)# key 1	Create key id 1
Switch(config-keychain-key)# key-string key1	Set password
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2012 14:00:00 Mar 7 2012	Set accept lifetime
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2012 12:00:00 Mar 7 2012	Set send lifetime
Switch(config-keychain-key)# exit	Exit
Switch(config-keychain)# key 2	Create key id 2
Switch(config-keychain-key)# key-string Earth	Set password
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2012 14:00:00 Mar 12 2012	Set accept lifetime
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 7 2012 12:00:00 Mar 12 2012	Set send lifetime
Switch(config-keychain-key)# end	Exit
Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# ip rip authentication key-chain SUN	Define interface authentication name
Switch(config-if)# ip rip authentication mode md5	Define interface authentication mode

III. Command validation

Use the following commands to validate the configuration above:

show running-config, show ip rip, show ip protocols rip, show ip rip interface and show key chain

Validate on Switch A

```
Switch# show key chain
```

```
key chain SUN:
   key 1 -- text "key1"
     accept-lifetime <12:00:00 Mar 02 2012> - <14:00:00 Mar 07 2012>
     send-lifetime <12:00:00 Mar 02 2012> - < 12:00:00 Mar 07 2012>
   key 2 -- text "Earth"
     accept-lifetime <12:00:00 Mar 07 2012> - <14:00:00 Mar 12 2012>
     send-lifetime <12:00:00 Mar 07 2012> - < 12:00:00 Mar 12 2012>
Switch#
```

Validate on Switch B

```
Switch# show key chain
key chain SUN:
   key 1 -- text "key1"
     accept-lifetime <12:00:00 Mar 02 2012> - <14:00:00 Mar 07 2012>
     send-lifetime <12:00:00 Mar 02 2012> - < 12:00:00 Mar 07 2012>
   key 2 -- text "Earth"
     accept-lifetime <12:00:00 Mar 07 2012> - <14:00:00 Mar 12 2012>
     send-lifetime <12:00:00 Mar 07 2012> - < 12:00:00 Mar 12 2012>
```

8.3 OSPF Configuration

8.3.1 Introduction

OSPF (Open shortest path first) is a link-state-based interior gateway protocol developed by IETF organization that supports IP subnetting and labeling external routes. The current version is version 2 (RFC2328), which has the following features:

- Scope of application: Support networks of all scales, and can support up to hundreds of routers.
- Rapid convergence: Send an update message immediately upon any change of the network topological structure, to realize synchronization of the change in the autonomous system.
- Loop-free: Since OSPF calculates the routing with the shortest path tree algorithm based on the collected link-state, it is ensured that no self-loop routing will be produced from the algorithm.
- Region partition: Allow the network of autonomous system to be partitioned for management, by which the routing information transmitted between the regions is further abstracted, so as to save bandwidth usage.
- Equal-cost routing: Supports multiple equal-cost routings to the same destination address.
- Routing classification: Four types of routing are adopted, including (ordered by priority): intra-area routing, inter-area routing, Class 1 external routing, and Class 2 external routing.
- Supported authentication: Interface-based message authentication for guaranteeing the security of routing computation.
- Multicast sending: Protocol messages are sent by means of multicast.

The current system supports the following OSPF features:

- **Supporting stub area:** Support routing redistribution, including importing the routes learned from other routing protocols into OSPF or the routes learned from OSPF into other routing protocols.
- **Supporting plaintext authentication and MD5 authentication:** Support the parameter configurations on OSPF interface, including output metric, retransmission time, send delay, router priority, router hello message interval, authentication key, and so on.
- Not supporting virtual links: Not support not-so-stubby area (NSSA)

  OSPF needs multiple routers for collaboration, including area border router (ABR), autonomous system border router (ASBR) and internal router. The simplest OSPF configuration can be completed by using the default parameters and adding all OSPF interfaces to a same area.

8.3.2 References

OSPF module is based on the following RFC:

RFC 2328 – OSPF version 2

8.3.3 Configure Basic OSPF

Create OSPF process on the router on which OSPF is to be enabled first, and specify the network segment to be released and area ID. The configuration is as below.

Switch# configure terminal	Enter configuration mode
Switch(config)# router ospf 100	Create OSPF process id as 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0. You can use netmask to add multiple interfaces into OSPF area
Switch(config-router)# end	Go back to configuration mode
Switch# show ip protocols	Check the configured protocols

Delete OSPF process with command "**no router ospf process-id**" in global mode.

Configure OSPF process id as 109 and distribute segment 131.108.0.0 to area 24:

Switch(config)# router ospf 109

Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24

8.3.4 Enable OSPF

This example shows the minimum configuration for enabling OSPF on an interface.

CAUTION

One interface can belong to one area only, and different interfaces can belong to different areas.

I. Topology

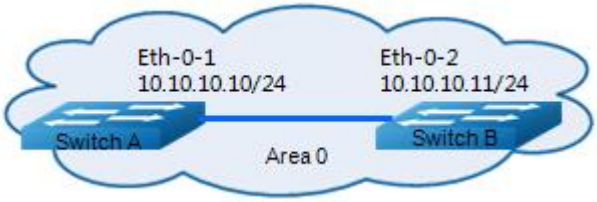


Figure 8-10 OSPF Autonomous System

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Configure interface eth-0-1
Switch(config-if)# ip address 10.10.10.10/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-2	Configure interface eth-0-2
Switch(config-if)# ip address 10.10.10.11/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 200	Create OSPF process id 200
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

III. Command validation

Use the following commands to validate the configuration above:

show ip ospf database, show ip ospf interface, show ip ospf neighborand show ip ospf route

Switch A

```
Switch# show ip ospf database
          OSPF Router with ID (10.10.10.10) (Process ID 100)
              Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.10.10     10.10.10.10     51 0x80000002 0xd012         1
Switch# show running-config router ospf
Building configuration...
!
router ospf 100
 network 10.10.10.0/24 area 0
!
```

Switch B

```
Switch# show ip ospf database
          OSPF Router with ID (10.10.10.10) (Process ID 200)
              Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.10.10     10.10.10.10     267 0x80000002 0xd012 1
Switch# show running-config router ospf
Building configuration...
!
router ospf 200
 network 10.10.10.0/24 area 0
!
```

8.3.5 Configure Priority

This example mainly shows how to configure interface priority. The interface of high priority becomes DR. Interfaces of 0 priority cannot be elected for DR. The priority of Switch C is 0, higher than the default priority (1) of Switch A and Switch B, so Switch C becomes the DR of the network.

I. Topology

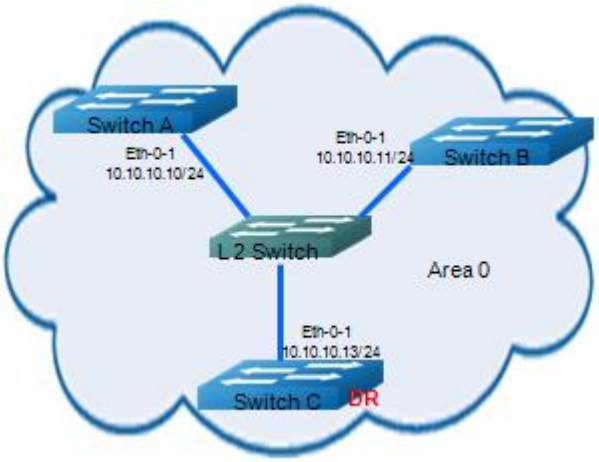


Figure 8-11 OSPF Priority

II. Configuration

Switch C

Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip ospf priority 10	Configure interface priority
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch B

Switch# configure terminal	Enter interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch A

Switch(config)# router ospf 200	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

III. Command validation

Use the following commands to validate the configuration above:

show ip ospf neighbor and show ip ospf interface

Switch C

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.10       1   Full/DROther    00:00:32    10.10.10.10     eth-0-1
10.10.10.11       1   Full/BDR        00:00:31    10.10.10.11     eth-0-1
Switch# show ip ospf interface
eth-0-10 is up, line protocol is up
  Internet Address 10.10.10.13/24, Area 0, MTU 1500
  Process ID 0, Router ID 10.10.10.13, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 10, TE Metric 1
  Designated Router (ID) 10.10.10.13, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.10.10.11, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 2, Adjacent neighbor count is 2
  Crypt Sequence Number is 1301567281
  Hello received 188 sent 110, DD received 34 sent 23
  LS-Req received 8 sent 6, LS-Upd received 28 sent 26
  LS-Ack received 32 sent 15, Discarded 0
```

8.3.6 Configure OSPF Area Parameters

You can configure several OSPE area parameters selectively. These parameters include authentication key for accessing unauthorized area and configuring an area as stub. Stub area refers to specific areas, the ABR of Stub area doesn't spread the autonomous system external routes they receive, and the routing table size and the quantity of routing information passing of routers in such areas will largely decrease. To make sure that the routes outwards the autonomous system are still reachable, the ABR in this area will generate a default route and distribute it to other non-ABR routers in the Stub area.

Route aggregation refers to ABR or ASBR aggregating routing information with the same prefix and sending one route to other areas only. After AS is partitioned into different areas, route aggregation can be utilized to reduce routing information and the size of routing table between the areas to increase the operating rate of routers. If the network numbers are consecutive, you can use the "area range" command to aggregate the consecutive network segments into one segment. By this, ABR will send an aggregated LSA only, and any other LSA within the aggregation network segment specified via this command will not be sent out separately, which can reduce LSDB size in other areas.

I. Topology

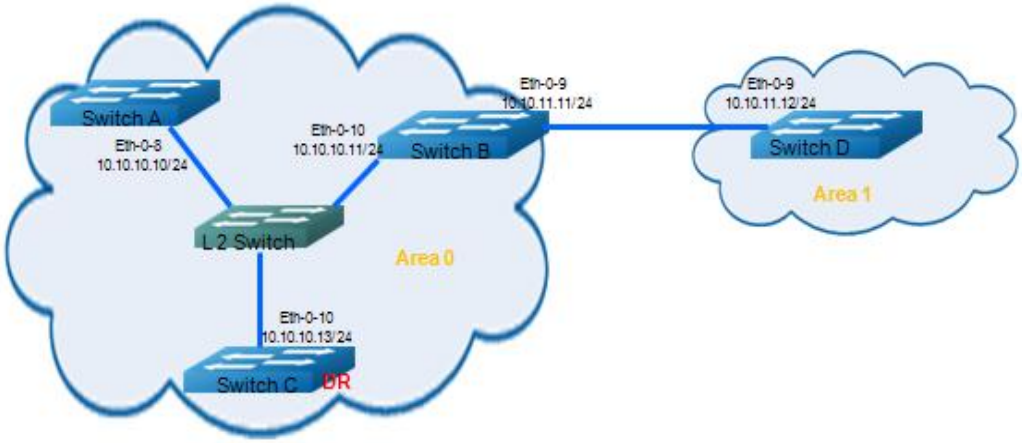


Figure 8-12 OSPF Area

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-8	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.10/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-10	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.11/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.11.11/24	Configure interface IP address
Swithc(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0
Switch(config-router)# network 10.10.11.0/24 area 1	Distribute 10.10.11.0/24 segment to OSPF area 1
Switch(config-router)# network 10.10.10.0/0 area 24	Assign an IP segment to distribute to OSPF area 0
Switch(config-router)# area 1 stub no-summary	Set area 1 as stub area
Switch(config-router)# end	Go back to configuration mode
Switch # show ip ospf 100 Switch # show ip ospf 100	Show OSPF 100 information

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-10	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.13/24	Configure interface IP address
Switch(config-if)# ip ospf priority 10	Set OSPF interface priority
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-9	Enter interface mode

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.11.12/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 200	Create OSPF process id 200
Switch(config-router)# network 10.10.11.0/24 area 1	Distribute 10.10.10.0/24 network segment to OSPF area 1
Switch(config-router)# area 1 stub no-summary	Set area 1 as stub area

III. Command validation

Use the “show ip route” command to validate the configuration above.

Switch A

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.10.0/24 is directly connected, eth-0-8
C      10.10.10.10/32 is in local loopback, eth-0-8
O IA   10.10.11.0/24 [110/2] via 10.10.10.11, eth-0-8, 00:14:46
```

Switch B

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C      10.10.10.0/24 is directly connected, eth-0-10
C      10.10.10.11/32 is in local loopback, eth-0-10
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.11/32 is in local loopback, eth-0-9
```

Switch C

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-10
C       10.10.10.13/32 is in local loopback, eth-0-10
O IA    10.10.11.0/24 [110/2] via 10.10.10.11, eth-0-10, 12:20:35 AM
```

Switch D

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
Gateway of last resort is 10.10.11.11 to network 0.0.0.0
O*IA    0.0.0.0/0 [110/2] via 10.10.11.11, eth-0-9, 00:12:46
C       10.10.11.0/24 is directly connected, eth-0-9
C       10.10.11.12/32 is in local loopback, eth-0-9
```

8.3.7 Configure OSPF Redistribution Route

Intra-area and inter-area routings describe the network structure inside AS, while external routing describes how to choose routing for reaching destination addresses other than AS. OSPF classifies the introduced AS external routing into Type1 and Type2.

Type1 refers to routes IGP (accepting interior gateway protocol), such as static route and RIP route. Since this type is of high credibility and is comparable to OSPF's routes in respect of cost, so the cost for reaching Type1 is equal to the sum of the cost from this router to corresponding ASBR and of that from the ASBR to this routing destination address.

Type2 refers to routes accepting EGP (exterior gateway protocol). Since this type is of low credibility, so OSPF protocols regard the cost from ASBR towards autonomous system is much higher than the cost for reaching ASBR within the autonomous system. Thus, the former will be primarily considered first, that's the cost for reaching Type2 is equal to the cost from ASBR to the routing destination address. If two routes with equal cost are calculated out, the cost from the router to corresponding ASBR can be considered. In the example below, RIP route will be redistributed into OSPF network as an external route.

I. Topology

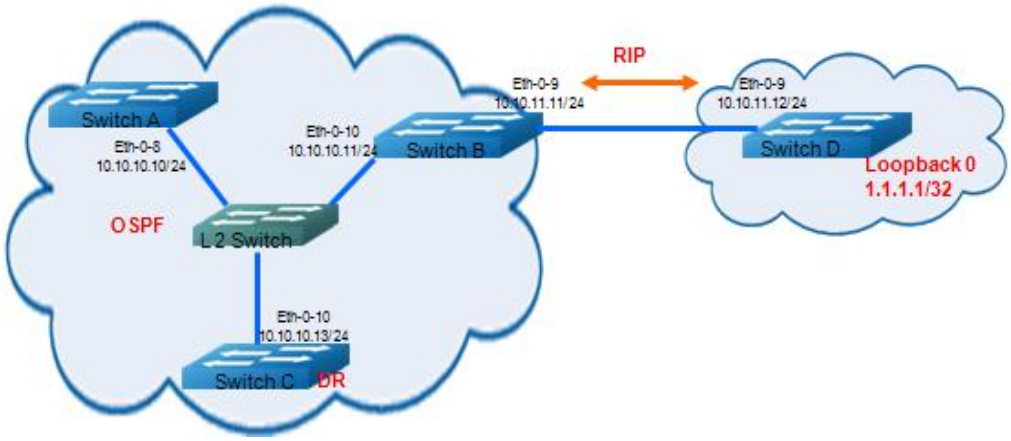


Figure 8-13 OSPF Route Redistribution

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-8	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.10/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-10	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.11/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface

Switch(config-if)# ip address 10.10.11.11/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0
Switch(config-router)# redistribute connected	Redistribute direct-connected route
Switch(config-router)#redistribute rip	Redistribution RIP route
Switch(config-router)# exit	Go back to configuration mode
Switch(config)# router rip	Create RIP route
Switch(config-router)# network 10.10.11.0/24	Distribute the network segment into RIP route
Switch(config-router)# redistribute connected	Redistribute direct-connected route

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-10	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.13/24	Set interface IP address
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0	Distribute 10.10.10.0/24 network segment to OSPF area 0

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.11.12/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router rip	Create RIP route

Switch(config-router)# network 10.10.11.0/24	Distribute the network segment into RIP routing
Switch(config-router)# network 1.1.1.1/32	Distribute the network segment into RIP routing
Switch(config-router)# redistribute connected	Redistribute direct-connected route

III. Command validation

Use the following commands to validate the configuration above:

show ip ospf database externa and show ip route

Switch A

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
O E2   1.1.1.1/32 [110/20] via 10.10.10.11, eth-0-8, 00:21:00
C      10.10.10.0/24 is directly connected, eth-0-8
C      10.10.10.10/32 is in local loopback, eth-0-8
O E2   10.10.11.0/24 [110/20] via 10.10.10.11, eth-0-8, 12:13:25 AM
Switch# show ip ospf database external
        OSPF Router with ID (10.10.10.10) (Process ID 100)
          AS External Link States
 LS age: 1447
 Options: 0x2 (*|-|-|-|-|-|E|-)
 LS Type: AS-external-LSA
 Link State ID: 1.1.1.1 (External Network Number)
 Advertising Router: 10.10.11.11
 LS Seq Number: 80000002
 Checksum: 0x414e
 Length: 36
 Network Mask: /32
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
 LS age: 993
 Options: 0x2 (*|-|-|-|-|-|E|-)
 LS Type: AS-external-LSA
 Link State ID: 10.10.11.0 (External Network Number)
 Advertising Router: 10.10.11.11
 LS Seq Number: 80000001
 Checksum: 0xfc78
```

```
  Length: 36
  Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

Switch B

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R      1.1.1.1/32 [120/2] via 10.10.11.12, eth-0-9, 00:24:52
C      10.10.10.0/24 is directly connected, eth-0-10
C      10.10.10.11/32 is in local loopback, eth-0-10
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.11/32 is in local loopback, eth-0-9
```

Switch C

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
         O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2
         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
         [*] - [AD/Metric]
         * - candidate default
O E2   1.1.1.1/32 [110/20] via 10.10.10.11, eth-0-10, 12:22:38 AM
C      10.10.10.0/24 is directly connected, eth-0-10
C      10.10.10.13/32 is in local loopback, eth-0-10
O E2   10.10.11.0/24 [110/20] via 10.10.10.11, eth-0-10, 12:15:04 AM
```

Switch D

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
         O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2
         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
         [*] - [AD/Metric]
         * - candidate default
C      1.1.1.1/32 is directly connected, loopback0
R      10.10.10.0/24 [120/2] via 10.10.11.11, eth-0-9, 12:17:36 AM
C      10.10.11.0/24 is directly connected, eth-0-9
C      10.10.11.12/32 is in local loopback, eth-0-9
```

8.3.8 Configure OSPF Cost

You can set an optimal routing by modifying the interface COST value. As shown in the example below, Switch B is made into the next hop of Switch A by modifying the COST value.

The default interface COST value is 1 (1000M speed). Eth-0-2 priority of Switch B is 100, and Eth-0-2 priority of Switch C is 150. Then, the Cost of reaching Switch D 10.10.14.0 will be different:

Switch B: 1+1+100 = 102

Switch C: 1+1+150 = 152

I. Topology

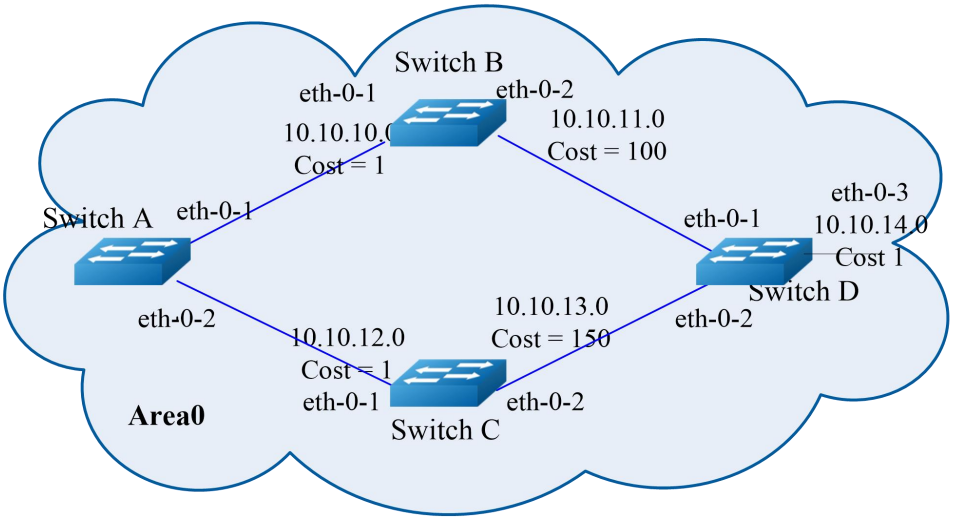


Figure 8-14 OSPF Cost

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode.
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.1/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.12.1/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode

Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.10.0/24 area 0 Switch(config-router)# network 10.10.12.0/24 area 0	distribute 10.10.10.0/24, 10.10.12.0/24 network segments to OSPF area 0

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.2/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.11.2/24	Configure interface IP address
Switch(config-if)# ip ospf cost 100	Set OSPF interface COST
Switch(config)# router ospf 100	Create OSPF process id 00
Switch(config-router)# network 10.10.10.0/24 area 0 Switch(config-router)# network 10.10.11.0/24 area 0	Distribute 10.10.10.0/24, 10.10.11.0/24 network segments to OSPF area 0

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.12.2/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.13.2/24	Configure interface IP address

Switch(config-if)# ip ospf cost 150	Set OSPF interface COST
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.12.0/24 area 0 Switch(config-router)# network 10.10.13.0/24 area 0	Distribute 10.10.10.0/24, 10.10.13.0/24 network segments to OSPF area 0

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.11.1/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.13.1/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-3	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.14.1/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf 100	Create OSPF process id 100
Switch(config-router)# network 10.10.11.0/24 area 0 Switch(config-router)# network 10.10.13.0/24 area 0 Switch(config-router)# network 10.10.14.0/24 area 0	Distribute 10.10.10.0/24, 10.10.13.0/24 network segments to OSPF area 0

III. Command validation

Use the “show ip ospf route” command to validate the configuration above.

Switch A

```
Switch# show ip ospf route
OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
C  10.10.10.0/24 [1] is directly connected, eth-0-1, Area 0
O  10.10.11.0/24 [101] via 10.10.10.2, eth-0-1, Area 0
C  10.10.12.0/24 [1] is directly connected, eth-0-2, Area 0
O  10.10.13.0/24 [102] via 10.10.10.2, eth-0-1, Area 0
O  10.10.14.0/24 [102] via 10.10.10.2, eth-0-1, Area 0
```

Switch B

```
Switch# show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
C  10.10.10.0/24 [10] is directly connected, eth-0-1, Area 0
C  10.10.11.0/24 [100] is directly connected, eth-0-2, Area 0
O  10.10.12.0/24 [11] via 10.10.10.1, eth-0-1, Area 0
O  10.10.13.0/24 [101] via 10.10.11.1, eth-0-2, Area 0
O  10.10.14.0/24 [101] via 10.10.11.1, eth-0-2, Area 0
```

Switch C

```
Switch# show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
O  10.10.10.0/24 [1] via 10.10.12.1, eth-0-1, Area 0
O  10.10.11.0/24 [101] via 10.10.12.1, eth-0-1, Area 0
C  10.10.12.0/24 [1] is directly connected, eth-0-1, Area 0
O  10.10.13.0/24 [102] via 10.10.12.1, eth-0-1, Area 0
O  10.10.14.0/24 [102] via 10.10.12.1, eth-0-1, Area 0
```

Switch D

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
O      10.10.10.0/24 [110/1] via 10.10.11.2, eth-0-1, 12:06:27 AM
C      10.10.11.0/24 is directly connected, eth-0-1
O      10.10.12.0/24 [110/1] via 10.10.13.2, eth-0-2, 12:06:17 AM
C      10.10.13.0/24 is directly connected, eth-0-2
C      10.10.14.0/24 is directly connected, eth-0-3
```

8.3.9 Configure OSPF Authentication

The system supports three types of OSPF authentication modes: No authentication (type 0), plaintext authentication (type 1) and MD5 authentication (type 2). No authentication refers to that no authentication is required for routing information exchange in the network. Plaintext authentication refers to that the authentication mode and key configured on all routers must be the same. MD5 authentication refers to that you must configure same key and key ID on every router. Routers will generate message digest based on key, key ID and OSPF message content and add it to OSPF message.

Authentication mode can be based on area configuration or interface configuration or both. If the configured interface authentication type is different from the configured area authentication type, the the interface authentication type is prior. If the interface is configured with no authentication type, then the area authentication type applies.

The example below briefs the three types of OSPF authentication. No authentication is assigned between Switch A and Switch B; plaintext authentication is assigned between Switch B and Switch A; DM5 authentication is assigned between Switch C and Switch D.

I. Topology

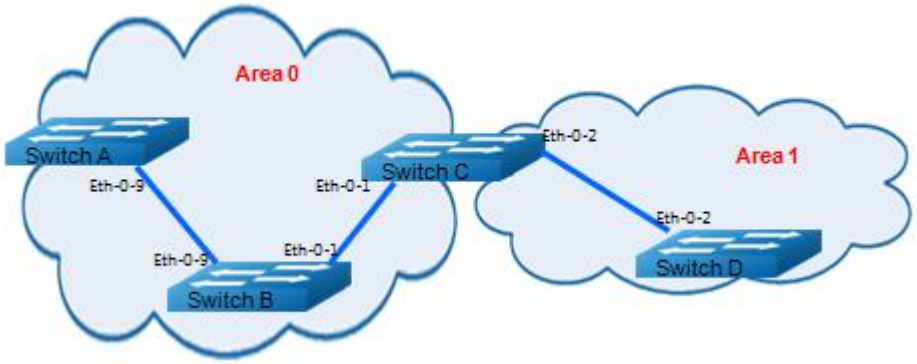


Figure 8-15 OSPF Authentication

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 9.9.9.1/24	Set IP address
Switch(config-if)#ip ospf authentication	Enable authentication on the interface
Switch(config-if)#ip ospf authentication null	Specify interface authentication type as null
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf	Create OSPF process

Switch(config-router)# network 9.9.9.0/24 area 0	Distribute network segment to OSPE
Switch(config-router)# end	Exit router mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 9.9.9.2/24	Set IP address
Switch(config-if)#ip ospf authentication	Enable authentication on the interface
Switch(config-if)#ip ospf authentication null	Specify interface authentication type as null
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 1.1.1.1/24	Set IP address
Switch(config-if)#ip ospf authentication	Enable plaintext authentication on the interface
Switch(config-if)# ip ospf authentication-key test	Specify interface authentication key
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf	Create OSPF process
Switch(config-router)# network 9.9.9.0/24 area 0 Switch(config-router)# network 1.1.1.0/24 area 0	Distribute network segment to OSPE
Switch(config-router)# end	Exit router mode

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-2	Enter interface mode

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 2.2.2.1/24	Set IP address
Switch(config-if)# ip ospf message-digest-key 2 md5 ospf	Set interface OSPF authentication key
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 1.1.1.2/24	Set IP address
Switch(config-if)#ip ospf authentication	Enable plaintext authentication on the interface
Switch(config-if)# ip ospf authentication-key test	Set interface OSPF authentication key
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf	Create OSPF process
Switch(config-router)# area 1 authentication message-digest Switch(config-router)# network 2.2.2.0/24 area 1 Switch(config-router)# network 1.1.1.0/24 area 0	Distribute network segment to OSPE, and configure authentication type of area1 as MD5
Switch(config-router)# end	Exit router mode

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 2.2.2.2/24	Set IP address
Switch(config-if)# ip ospf message-digest-key 2 md5 ospf	Set interface OSPF authentication key
Switch(config-if)# exit	Exit interface mode
Switch(config)# router ospf	Create OSPF process

Switch(config-router)# area 1 authentication message-digest Switch(config-router)# network 2.2.2.0/24 area 1	Distribute network segment to OSPE, and configure authentication type of area1 as MD5
Switch(config-router)# end	Exit router mode

III. Command validation

Use the "**show ip ospf neighbor**" command to validate the configuration above.

Switch A

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.2           1   Full/DR         00:00:38    9.9.9.2         eth-0-9
```

Switch B

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.1           1   Full/Backup     00:00:35    1.1.1.2         eth-0-1
1.1.1.1           1   Full/Backup     00:00:38    9.9.9.1         eth-0-9
```

Switch C

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.2           1   Full/DR         00:00:35    1.1.1.1         eth-0-1
2.2.2.2           1   Full/DR         12:00:38 AM    2.2.2.2         eth-0-2
Switch# show ip ospf interface
eth-0-1 is up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0, MTU 1500
  Process ID 0, Router ID 2.2.2.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 9.9.9.2, Interface Address 1.1.1.1
  Backup Designated Router (ID) 2.2.2.1, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 12:00:01 AM
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 1301244696
  Hello received 385 sent 384, DD received 3 sent 5
  LS-Req received 1 sent 1, LS-Upd received 11 sent 14
  LS-Ack received 12 sent 10, Discarded 1
  Simple password authentication enabled
Switch# show ip ospf
 Routing Process "ospf 0" with ID 2.2.2.1
 Process uptime is 1 hour 7 minutes
 Process bound to VRF default
```

```
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 17
Number of LSA received 57
Number of areas attached to this router: 2
  Area 0 (BACKBONE)
     Number of interfaces in this area is 1(1)
     Number of fully adjacent neighbors in this area is 1
     Area has no authentication
     SPF algorithm last executed 01:06:56.340 ago
     SPF algorithm executed 16 times
     Number of LSA 6. Checksum 0x034b09
  Area 1
     Number of interfaces in this area is 1(1)
     Number of fully adjacent neighbors in this area is 1
     Number of fully adjacent virtual neighbors through this area is 0
     Area has message digest authentication
     SPF algorithm last executed 12:03:29 AM.430 ago
     SPF algorithm executed 17 times
     Number of LSA 5. Checksum 0x0230e3
```

Switch D

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State          Dead Time   Address         Interface
2.2.2.1           1   Full/Backup    12:00:35 AM    2.2.2.1         eth-0-2
```

8.3.10 Configure Listening OSPF

You can run commands to show detailed statistics, such as the content of IP routing table, cache and database.

Switch # show ip ospf 100	Show OSPF process information

Switch # show ip ospf 100 database router 10.10.25.21 adv-router 3.3.3.3 Switch # show ip ospf 100 database network self-originate Switch # show ip ospf 100 database summary Switch # show ip ospf 100 database asbr-summary Switch # show ip ospf 100 database external	Show OSPF link status information base
Switch # show ip ospf border-routes	Show OSPF information of border router
Switch # show ip ospf interface eth-0-1	Show OPSF interface information
Switch # show ip ospf neighbor 172.16.12.100	Show OSPF neighbor information

8.4 Prefix-list Configuration

8.4.1 Introduction

Routing policy is a technology of modifying routing information to change the path of network traffic, which is mainly realized by changing routing attributes (including reachability). Address prefix list is one routing policy, which can be flexibly applied. Address prefix list is identified via prefix list name. An address prefix list can contain multiple entries, each entry can individually specify a match range identified with index number in the form of network prefix. The index number indicates the order of match check. In matching process, switches check entries identified with index number by ascending order. The matching process will end once an entry meets the conditions, and the matching of next entries will not continue.

8.4.2 Basic Configuration

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip prefix-list test seq 1 deny 35.0.0.0/8 le 16	Create address prefix list test, and create an entry numbered 1
Switch(config)# ip prefix-list test permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# ip prefix-list test description this prefix list is fot test	Add address prefix list description
Switch(config)# ip prefix-list test permit 36.0.0.0/24	Create an entry numbered with a default serial number
Switch(config)# exit	Exit global mode

II. Command validation

Switch# show ip prefix-list detail

```
Prefix-list list number: 1
Prefix-list entry number: 3
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
  Description: this prefix list is fot test
  count: 3, range entries: 0, sequences: 1 - 10
    seq 1 deny 35.0.0.0/8 le 16 (hit count: 0, refcount: 0)
    seq 5 permit any (hit count: 0, refcount: 0)
    seq 10 permit 36.0.0.0/24 (hit count: 0, refcount: 0)
```

8.4.3 Configure Rip Simple Application

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16	Create address prefix list aa, and create an entry
Switch(config)# ip prefix-list aa permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# router rip	Enter Rip router mode
Switch(config-router)# distribute-list prefix aa out	Apply policy
Switch(config-router)# end	Exit Rip router mode

II. Command validation

Switch# show ip prefix-list

```
ip prefix-list aa: 2 entries
    seq 11 deny 35.0.0.0/8 le 16
    seq 15 permit any
Switch# show running-config
Building configuration...
…
ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16
ip prefix-list aa seq 15 permit any
…
router rip
 distribute-list prefix aa out
```

8.4.4 Configure Route-map Simple Application

I. Configure applying prefix-list to route-map

Switch# configure terminal	Enter configuration mode
Switch(config)# ip prefix-list aa seq 11 deny 3.3.3.0/8 le 24	Create address prefix list aa, and create an entry
Switch(config)# ip prefix-list aa permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# route-map abc permit	Create route-map
Switch(config-route-map)# match ip address prefix-list aa	Match address prefix list aa
Switch(config-route-map)# set local-preference 200	Set actions
Switch(config-route-map)# exit	Exit router mode
Switch(config)# route-map abc permit 20	Redefine a policy to avoid being denied in the case of unmatched entry
Switch(config-route-map)# exit	Exit router mode
Switch(config)# router bgp 1	Enter BGP router mode
Switch(config-router)# neighbor 1.1.1.2 remote-as 1	Configure BGP neighbor
Switch(config-router)# neighbor 1.1.1.2 route-map abc out	Apply routing policy to BGP route
Switch(config-router)# network 2.2.2.2/32	Declare network segment in BGP route
Switch(config-router)# network 3.3.3.3/32	Declare network segment in BGP route
Switch(config-router)# end	Exit BGP mode

II. Command validation

Switch # show route-map

```
route-map abc, permit, sequence 10
  Match clauses:
    ip address prefix-list aa
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
Set clauses:
Switch # show running-config
Building configuration...
```

```
…
ip prefix-list aa seq 11 deny 3.3.3.0/8 le 24
ip prefix-list aa seq 15 permit any
!
!
route-map abc permit 10
 match ip address prefix-list aa
 set local-preference 200
!
route-map abc permit 20
…
router bgp 1
 neighbor 1.1.1.2 remote-as 1
 !
 address-family ipv4
 no synchronization
 network 2.2.2.2 mask 255.255.255.255
 network 3.3.3.3 mask 255.255.255.255
 neighbor 1.1.1.2 activate
 neighbor 1.1.1.2 route-map abc out
 exit-address-family
 !
 address-family vpnv4 unicast
 no synchronization
 exit-address-family
```

8.5 Route-map Configuration

8.5.1 Introduction

Routing policy is a technology of modifying routing information to change the path of network traffic, which is mainly realized by changing routing attributes (including reachability).

Routers might need to exercise some policies while releasing and accepting routing information, so as to filter routing information, such as accepting or releasing routing information meeting certain conditions only. A routing protocol may need to introduce routing information discovered by other routing protocols, routers may need to introduce the part meeting the conditions when introducing routing information of other routing protocols only and control some attributes of the introduced routing information to make it meet the requirements of the protocol. To realize routing policy, the first step is to define the features of routing information on which routing policy is to be exercised, namely a set of matching rules. Setting up can be made based on various attributes contained in routing information as matching rule, such as destination address, address of router releasing routing information. Matching rules can be pre-established, and then applied to the routing policy for routing distributing, accepting and introducing.

8.5.2 Configure Route-map Application to OSPF

I. Configuration

DUT# configure terminal	Enter configuration mode
DUT(config)# route-map abc permit	Create a routing policy
DUT(config-route-map)# match metric 20	Establish rules
DUT(config-route-map)# set tag 2	Set actions
DUT(config-route-map)# exit	Exit policy mode
DUT(config)# route-map abc permit 20	Redefine a policy to avoid being denied in the case of unmatched entry
DUT(config-route-map)# exit	Exit policy mode
DUT(config)# router ospf 100	Enter OSPF router mode
DUT(config-router)# redistribute rip route-map abc	Redistribute RIP protocol to OSPF, and apply policy abc
DUT(config-router)# end	Exit OSPF routing mode

II. Command validation

Switch# show route-map

```
route-map abc, permit, sequence 10
  Match clauses:
    metric 20
  Set clauses:
    tag 2
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
```

8.5.3 Configure Route-map Application to BGP

I. Configuration

Command	**Description**
DUT# configure terminal	Enter configuration mode
DUT(config)# ip access-list acl1	Create an ACL
DUT(config-ip-acl)# permit any 3.3.3.0 0.0.0.255 any	Set matching entries
DUT(config-ip-acl)# exit	Exit ACL mode

DUT(config)# route-map abc permit	Establish routing policy
DUT(config-route-map)# match ip address acl1	Match ACL
DUT(config-route-map)# set local-preference 200	Set actions
DUT(config-route-map)# exit	Exit router mode
DUT(config)# route-map abc permit 20	Redefine a policy to avoid being denied in the case of unmatched entry
DUT(config-route-map)# exit	Exit router mode
DUT(config)# router bgp 1	Enter BGP router mode
DUT(config-router)# neighbor 1.1.1.2 remote-as 1	Configure BGP neighbor
DUT(config-router)# neighbor 1.1.1.2 route-map abc out	Apply routing policy to BGP route
DUT(config-router)# network 2.2.2.2/32	Declare network segment in BGP route
DUT(config-router)# network 3.3.3.3/32	Declare network segment in BGP route
DUT(config-router)# end	Exit BGP mode

II. Command validation

DUT1# show route-map

```
route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
DUT2# show ip bgp
BGP table version is 6, local router ID is 1.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i2.2.2.2/32       1.1.1.1                  0    100      0 i
*>i3.3.3.3/32       1.1.1.1                  0    200      0 i
```

8.6 Policy-based Routing (PBR) Configuration

8.6.1 Introduction

Different from forwarding solely based on IP message destination address, policy-based routing is a mechanism of routing and forwarding based on user-established policy.

8.6.2 Topology

The figure below shows a typical configuration of policy-based routing: you can apply a PBR on eth-0-1 of Switch, messages with a source address of 172.16.6.1 will be forwarded to Lucy, and messages with a source address of 172.16.7.1 will go through normal routing transfer.

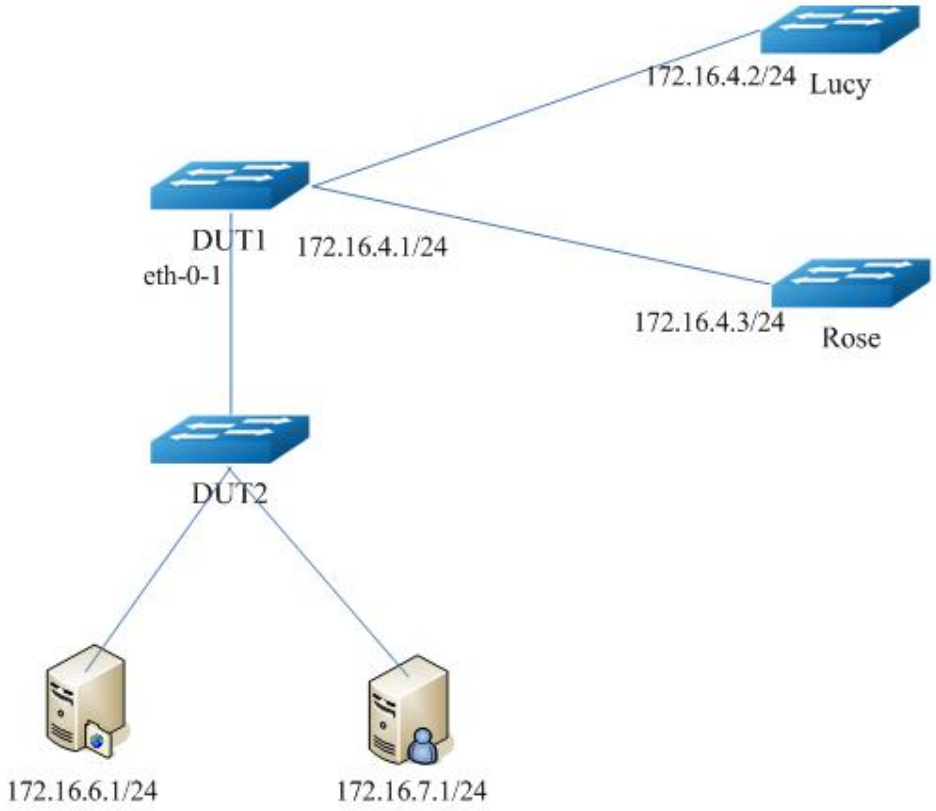


Figure 8-16 Typical PBR Topology

8.6.3 Configuration

DUT# configure terminal	Enter configuration mode
Switch(config)# ip access-list acl1	Define an IPV4 ACL and enter ACL configuration mode

Switch(config-ip-acl)# 10 permit any 172.16.6.0 0.0.0.255 any	Configure an ACE to permit messages with source address of 172.16.6.0
Switch(config-ip-acl)# exit	Exit ACL configuration mode
Switch(config)# route-map richard permit 10	Create a route-map named Richard and enter route-map configuration mode
Switch(config-route-map)# match ip address acl1	Configure a match sentence of match acll
Switch(config-route-map)# set ip next-hop 172.16.4.2	Set the forwarding address of data packets meeting the conditions as 172.16.4.2
Switch(config-route-map)# exit	Exit Route-map configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# ip address 172.16.5.2/24	Configure interface IP address
Switch(config-if)# no shutdown	Enable this interface
Switch(config-if)# ip policy route-map richard	Apply richard policy on the interface
Switch(config-if)# exit	Exit interface configuration mode

8.6.4 Command Validation

Switch# show ip policy route-map

Route-map	interface
richard	eth-0-1

8.7 BGP Configuration

8.7.1 Introduction

Border gateway protocol (BGP) is an internal autonomous system routing protocol.

The major function of BGP notification system is to exchange other BGP systems with reachable information on the network. The reachable network information includes reachable information in autonomous system. This information is sufficient for establishing a connectable

AS (it will be cut in the case of routing loops, and some policies will be forcibly executed at the level of this AS).

BGP-4 provides a set of mechanisms to support classless inter-domain routing (CIDR) [RFC1518, RFC1519]. These mechanisms include releasing a set of IP prefix source addresses, which has eliminated the concept of "Class" in BGP. BGP-4 also has introduced some concepts of allowed routing sets (including AS path sets).

The routing information exchanged by BGP supports destination-based examples only, assuming routers forward messages via the destination address in IP message header only. In turn, it causes whether BGP can be forcibly applied to these policy decisions. BGP can support policies forwarded based on destination address.

Please refer to [RFC 1771, RFC 4271] for detailed BGP information.

8.7.2 Basic Topology (EBGP)

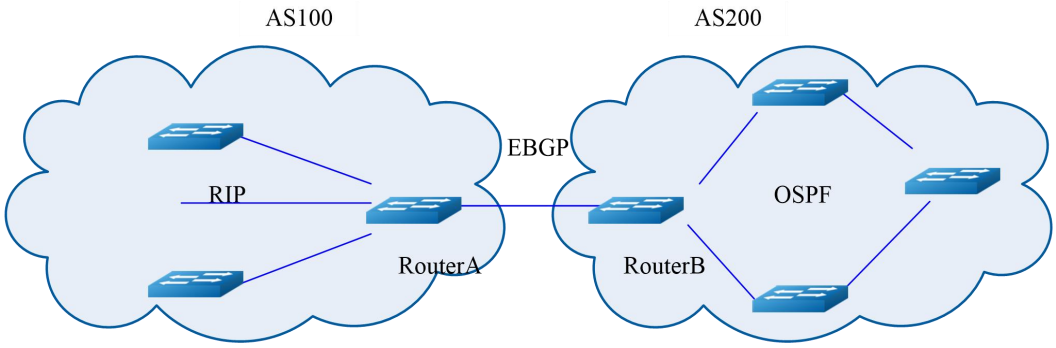


Figure 8-17 EBGP Topology

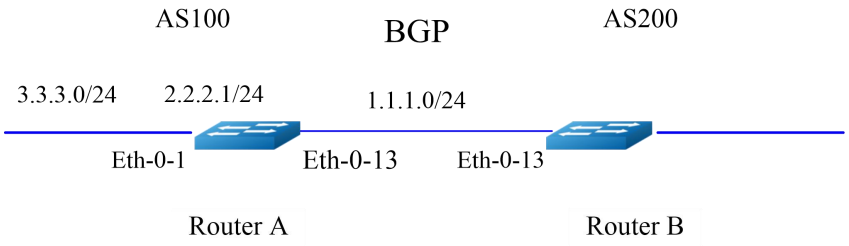


Figure 8-18 EBGP Topology

I. Configuration

Router A

Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface.
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.

Switch(config-if)# ip address 1.1.1.1/24	Configure IP address 1.1.1.1/24.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# interface eth-0-1	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface.
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.
Switch(config-if)# ip address 2.2.2.1/24	Configure IP address 2.2.2.1/24.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# ip route 3.3.3.0/24 2.2.2.2	Add a static route.
Switch(config)# router bgp 100	Create BGP 100 and enter route mode.
Switch (config-router)#bgp router-id 10.10.10.10	Configure BGP router-id.
Switch(config-router)# neighbor 1.1.1.2 remote-as 200	Configure EBGP neighbor number as 200.
Switch (config)# neighbor 1.1.1.2 ebgp-multihop	Configure neighbor as ebgp-multihop.
Switch(config-router)# network 4.0.0.0/8	Declare network number.
Switch(config-router)# redistribute static	Redistribute static route to BRP.
Switch(config-router)# redistribute connected	Redistribute direct-connected route to BGP.
Switch(config-router)# exit	Exit router mode and enter configuration mode.

Router B

Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface.
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.
Switch(config-if)# ip address 1.1.1.2/24	Configure IP address 1.1.1.2/24.

Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# router bgp 200	Create BGP 200 and enter route mode.
Switch (config-router)#bgp router-id 11.11.11.11	Configure BGP router-id.
Switch(config-router)# neighbor 1.1.1.1 remote-as 100	Configure EBGP neighbor number as 100.
Switch (config)# neighbor 1.1.1.1 ebgp-multihop	Configure neighbor as ebgp-multihop.
Switch(config-router)# redistribute connected	Redistribute direct-connected route to BGP.
Switch(config-router)# exit	Exit route mode and enter configuration mode.

II. Test Results

SwitchA# show ip bgp neighbors

```
BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read 12:26:00 AM, hold time is 180, keepalive interval is 60 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 0
 Index 1, Offset 0, Mask 0x2
 0 accepted prefixes
 0 announced prefixes
Connections established 0; dropped 0
 External BGP neighbor may be up to 255 hops away.
```

Next connect timer due in 87 seconds

```
SwitchB# show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read 12:21:39 AM, hold time is 180, keepalive interval is 60 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 0
 Index 1, Offset 0, Mask 0x2
```

0 accepted prefixes
0 announced prefixes
Connections established 0; dropped 0
External BGP neighbor may be up to 255 hops away.
Next connect timer due in 97 seconds

8.7.3 Basic Topology (IBGP)

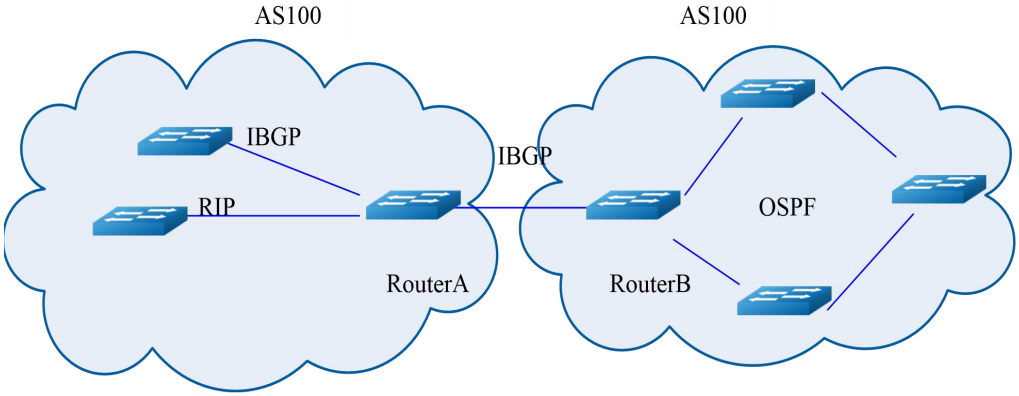


Figure 8-19 IBGP

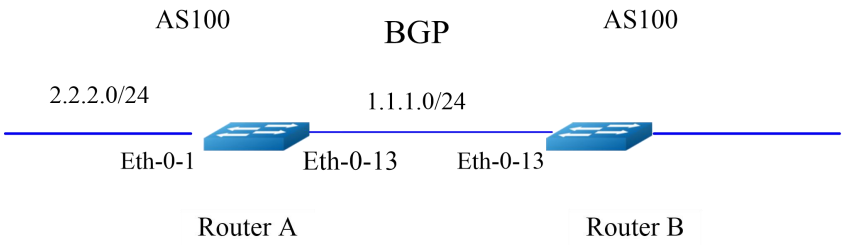


Figure 8-20 IBGP Topology

I. Configuration

Router A

Switch #configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface.
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.
Switch(config-if)# ip address 1.1.1.1/24	Configure IP address 1.1.1.1/24.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# interface loopback 0	Enter interface mode.

Switch(config-if)# ip address 10.10.10.10/32	Configure IP address as 12.1.1.1/32.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# ip route 11.11.11.11/32 1.1.1.2	Add a static route.
Switch(config)# interface eth-0-1	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.
Switch(config-if)# ip address 2.2.2.1/24	Configure IP address 2.2.2.1/24.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# ip route 3.3.3.0/24 2.2.2.2	Add a static route.
Switch(config)# router bgp 100	Create BGP 100 and enter route mode.
Switch (config-router)#bgp router-id 10.10.10.10	Configure BGP router-id.
Switch(config-router)# neighbor 11.11.11.11 remote-as 100	Configure IBGP neighbor number as 100.
Switch (config-router)#neighbor 11.11.11.11 update-source loopback 0	Configure loopback0 as update source interface.
Switch(config-router)# network 4.0.0.0/8	Declare network number.
Switch(config-router)# redistribute static	Redistribute static route to BRP.
Switch(config-router)# redistribute connected	Redistribute direct-connected route to BGP.
Switch(config-router)# exit	Exit route mode and enter configuration mode.

Router B

Switch #configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode.
Switch(config-if)# no shutdown	Enable the interface.
Switch(config-if)# no switchport	Convert the interface to Layer 3 interface.

Switch(config-if)# ip address 1.1.1.2/24	Configure IP address 1.1.1.2/24.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# interface loopback 0	Enter interface mode.
Switch(config-if)# ip address 11.11.11.11/32	Configure IP address as 11.11.11.11/32.
Switch(config-if)# exit	Exit interface mode and enter configuration mode.
Switch(config)# ip route 10.10.10.10/32 1.1.1.1	Add a static route.
Switch(config)# router bgp 100	Create BGP 100 and enter route mode.
Switch (config-router)#bgp router-id 11.11.11.11	Configure BGP router-id.
Switch(config-router)# neighbor 10.10.10.10 remote-as 100	Configure IBGP neighbor number as 100.
Switch (config-router)#neighbor 10.10.10.10 update-source loopback 0	Configure loopback0 as update source interface.
Switch(config-router)# redistribute connected	Redistribute direct-connected route to BGP.
Switch(config-router)# exit	Exit route mode and enter configuration mode.

II. Test Results

SwitchA# show ip bgp neighbors

```
BGP neighbor is 11.11.11.11, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read 12:02:32 AM, hold time is 180, keepalive interval is 60 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 5 seconds
 Update source is loopback0
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 0
 Index 1, Offset 0, Mask 0x2
 0 accepted prefixes
 0 announced prefixes
 Connections established 0; dropped 0
Next connect timer due in 62 seconds
SwitchB# show ip bgp neighbors
```

```
BGP neighbor is 10.10.10.10, remote AS 100, local AS 100, internal link
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read 12:01:58 AM, hold time is 180, keepalive interval is 60 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 5 seconds
 Update source is loopback0
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 0
 Index 1, Offset 0, Mask 0x2
 0 accepted prefixes
 0 announced prefixes
Connections established 0; dropped 0
Next connect timer due in 17 seconds
```

9 Flow Management Guide

9.1 QoS Configuration

9.1.1 Introduction

QoS (Quality of Service) is a concept for evaluating the ability of service providers to meet customers service needs, widely involved in occasions of service supply and demand. Evaluation generally is not an exact mark, but is to lay emphasis on analyzing the attainments and defects so as to make improvement accordingly. In the Internet, QoS is for evaluating the capability of network packet delivery. Since the network provides diverse services, QoS evaluation can be performed on different bases. The QoS commonly mentioned refers to evaluation on the capability of supporting the core requirements for delay, delay jitter and packet loss probability in the process of packet delivery. QoS is a network security mechanism and technology for solving issues including network delay and congestion. In normal circumstances, if a network is applied to specific timeless application system only, QoS is not needed, such as Web application or E-mail setting, etc. Yet QoS is essential to key applications and multimedia application. In the case of network overload or congestion, QoS can ensure significant traffic from delay or discarding and guarantee high-efficiency network running.

9.1.2 Terms

The below briefs the terms and concepts related to QoS:

Access Control List (ACLs)

Classify traffic with the same characteristics. IP ACL is used for classifying IP traffic, and MAC ACL for all traffic types other than IPV6 and MPLS.

Class of Service (CoS)

A field for determining message priority on layer 2 of network. QOS can differentiate traffic classes by priority by setting COS value. 802.1Q layer 2 messages could carry 2-byte VLAN tag, and up to 3 bit is for user-assigned priority. Messages of other types could not carry VLAN tag. CoS is 3-bit, and its value range is between 0 and 7.

Differentiated Services Code Point (DSCP)

It is 6-bit and for differentiating message priority in layer 3 network. The range of DSCP value is 0-63.

IP-Precedence

It is 3-bit and for differentiating message priority in layer 3 network. The range of IP-Precedence value is 0-7.

EXP

It is 3-bit and for differentiating message priority in MPLS network. The range of MPLS EXP value is 0-7.

Traffic Classification

Identify messages fit certain characteristics by specific rules. Classification rule refers to filtering rule established by users based on the management requirements. Once a message enters the system, the traffic classification processing engine will assign an internal priority to it, and the system will process it as necessary based on the priority. The system could base on the CoS, inner-CoS, DSCP or IP-Precedence in messages, the configured default CoS of ports, or the mapped internal priority based on policy-map configurations.

Traffic Shaping

A method for adjusting ingress traffic rate via cache message to make the egress traffic rate more smooth. In the case of advanced burst of ingress traffic, it is needed to cache messages and send later to make the egress traffic more smooth. By this, shaping might increase packet jitter.

Traffic shaping can be applied to:

- Physical port shaping
- Egress queue shaping

In the event that double-rate shaping is applied to queue, it must be ensured that the sum of all queue CIRs is not larger than the port rate as well as the shaping rate of port.

Traffic Policing

Measure the traffic rate to determine whether a packet remains within the guaranteed rate or not. The traffic out of the guaranteed rate might be discarded.

The system supports two types of policer:

- Be configured in class-map, and limit the bandwidth of traffic matching certain class-map.
- Configure an aggregation policer, so that users can add traffic mating the class-map into the policer. Aggregation policer limits the bandwidth of all flows in it.

Marking

Define processing action on traffic out of the guaranteed rate. The system employs one of the two actions: color-mark packets for processing later; discard packets.

Marking can be performed both in ingress and egress directions.

Queueing

Each egress port in basic and enterprise modes has 8 queues with a range of 0-7. The highest priority is 7, and the lowest is 0. Each egress port in enterprise advance mode has 12 queues with a range of 0-11. 0-7 relates to unicast traffic queues, and 8-11 to multicast traffic queues. Among the unicast traffic queues, the highest priority is 7, and the lowest is 0. Among the multicast traffic queues, the highest priority is 11, and the lowest is 8. Each queue supports 3 discard priorities. Queue length is in the unit of buffer cell. Buffer cell is the unit of packet storage granularity (equal to 256 bytes). Large packet occupies more buffer cell.

Tail Drop

A simple drop algorithm, namely dropping the following packets once the packets in the queue reach a certain threshold (configurable). By default, tail drop is applied to interface. The system supports defining a tail drop threshold for every drop priority of each queue of each port.

WRED (Weighted Random Early Detection)

WRED (weighted random early detection) allows to drop packets early with certain probability to avoid congestion. The early drop of WRED mode helps avoiding a mass of packet drop within a short time that will result in a large amount of TCP connections and trigger slow start and congestion avoidance to instantly reduce network bandwidth utilization. The system supports defining two thresholds for every drop priority of each queue on ports, with the first one less than the second one. Packet drop starts once the packets reaches the first threshold. A large amount of packets results in a large drop probability. All packets are dropped once the second threshold is exceeded.

Scheduling

The system assigns a priority for each queue with a range of 0-7. Large number means high priority. The priority of the 8 queues of port in basic mode is assignable.

With QoS enabled, the priority of the queues in basic mode corresponding to the range of 0-7 is: 0/1/2/3/4/5/6/7; the priority of the queues in enterprise mode corresponding to the range of 0-7 is: 3/3/4/4/4/4/5/7; the priority of the queues in enterprise advance mode corresponding to the range of 0-11 is: 3/3/4/4/4/4/5/7/0/1/2/3.

With QoS disabled, the priority of all queues is 0.

On a port, SP is employed for scheduling different priorities, namely scheduling high priority queues first, and then scheduling low priority queues if high priority queues are null. For scheduling queues of the same priority, WDRR is applied. Users can set a weight for each queue.

With QoS enabled, the WDRR weight of the queues in basic mode corresponding to the range of 0-7 is: 1::1:1:1:1:1:1:1; the WDRR weight of the queues in enterprise mode corresponding to the range of 0-7 is: 1:1:4:10:10:10:1:1; the WDRR weight of the queues in enterprise advance mode corresponding to the range of 0-11 is: 1:1:4:10:10:10:1:1:1:1:1:1

Class Map

Define a set of flows by specifying ACLs. The ACLs can be match-all or match-any, which means flows matching all ACLs or any ACL respectively.

Policy Map

Be used to specify behaviors of traffic of different types to realize the following needs:

- Differentiate traffic by specific priority and color
- Establish a trust policy for corresponding priority and color settings
- Perform policing on traffic meeting certain trust policy in accordance with pre-configurations
- Redirect specific traffic
- Mirror specific traffic
- Make statistics of specific traffic

Policy Map has the following attributes:

- One policy map can contain multiple traffic classification definitions and perform individual actions
- One traffic classification definition matches one traffic type on interface
- Only one policy map can be applied in each direction of each interface. A policy map can be applied in different directions of different interfaces.
- Policy map must be attached to a port to come into force.
- A policy map can be applied to physical ports (non-aggregate port member), aggregate port and VLAN interface.

Mapping Tables

During QoS processing, the system maps all traffics to the internal priority for processing.

- For traffic classification, QoS performs message mapping via configurable mapping tables. The internal priority is 6-bit, and is mapped from CoS, EXP, DSCP and IP-Precedence values. The mapping tables include CoS-Priority-Color/COS-PHB, EXP-Priority-Color/EXP-PHB, DSCP-Priority-Color/DSCP-PHB and IP-Precedence-Priority-Color/IP-PREC-PHB.
- For traffic policing, QoS assigns a new priority and color for packets, such as basing on Class-Map.
- Once traffic scheduling is completed, if CoS is replaced or DSCP is put aside, then QoS employs Priority-Color-Cos/PHB-COS or Priority-Color-DSCP/PHB-DSCP to remap to CoS or DSCP based on the internal priority and color
- The aforementioned actions differ from QoS domain to QoS domain

Time-range

With Time-Range, Class-Map action can be enabled or disabled at a specific time set on weekly basis. Name Time-Range, define a Time-Range on a weekly basis, and apply it to ACE.

Time-Range can be used to set an individual ACE of Class-Map at a specific time on weekly basis.

RTCM

Single Rate Three Color Marker

TRTCM

Two Rate Three Color Marker

CIR

Committed Information Rate

CBS

Committed Burst Size

EBS

Excess Burst Size

PIR

Peak Information Rate

9.1.3 Modular QoS Command Line

Classify ingress traffic based on QoS policy.

Class-map QoS

Be used for defining a set of flows according to the rules of CoS/DSCP/IP Precedence/EXP/ACL.

Policy-map QoS

Be used for classifying traffic types. Policy-maps of the same type are associated with the same class-map QoS.

Class-map Priority

Be used for defining traffic priority.

Policy-map Priority

Be used for classifying QoS traffic policing. Policy-maps of the same type are associated with the same class-map traffic classification.

9.1.4 Configuration Guide

The following knowledge is required for configuring QOS:

- QoS policing cannot be configured on LinkAGG.
- Classification can be performed in the ingress direction only.
- Class map can contain multiple ACLs, and each ACL can contain multiple entries.
- Policing cannot be applied to virtual interface of switches.

9.1.5 Topology

Figure 9-1 Switch

9.1.6 Configuration

I. Configure egress queues

Tail Drop

Tail drop is a default congestion avoidance technology for egress queues. Messages will be cached in queue until exceeding the queue length.

The example below shows how to configure tail drop thresholds for various drop priorities.

- configure terminal;
- Create class-map priority, and specify the priority;
- Create policy-map priority, and make association with the class-map previously defined;
- Set the upper tail drop limit of the priority in policy-map priority mode;
- Interface IFNAME enters the interface matching corresponding policy table. IFNAME is the interface name.

The example below shows steps of configuring upper tail drop limit for traffic priority 3, where the upper tail drop limit is 2000.

Table 9-1 Configure Tail Drop

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map type traffic-class tc3	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 3	Set traffic priority 3
Switch(config-cmap-)# exit	Exit the configuration mode

Switch(config)# policy-map type traffic-class tc	Create policy-map and enter its configuration mode
Switch(config-pmap-tc)# class type traffic-class tc3	Make association with class-map
Switch(config-pmap-tc-c)# queue-limit 2000	Configure upper packet drop limit as 2000
Switch(config-pmap-tc-c)# exit	Exit configuration mode
Switch(config-pmap-tc)# exit	Exit to global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# service-policy type traffic-class tc	Apply QoS policy
Switch(config-if)# end	Exit global configuration mode
Switch# show qos interface eth-0-1 egress	Show QoS configuration

Configuration Verification

Switch# show qos interface eth-0-1 egress

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Max-Queue-Limit(Cell)	ECN
0	0	-	-	dynamic	level 0	-
1	0	-	-	dynamic	level 0	-
2	0	-	-	dynamic	level 0	-
3	0	-	-	tail-drop	2000	2000
4	0	-	-	dynamic	level 0	-
5	0	-	-	dynamic	level 0	-
6	0	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

WRED

WRED drops portion of packets selectively to reduce the probability of tail drop in the case of interface congestion. By dropping portion of packets selectively in early stage rather than starting drop at the time the queue is full, WRED can avoid synchronous TCP packet loss, so as to increase network throughput.

The example below shows how to configuring WRED thresholds for messages in different colors.

- configure terminal
- Create class-map priority, and specify the priority;
- Create policy-map priority, and make association with the class-map previously defined;
- Specify the upper WRED drop limit of the priority in policy-map priority mode;
- Interface IFNAME enters the interface matching the corresponding policy table. IFNAME is the interface name.

The example below shows steps of setting upper WRED drop limit for traffic priority 1. The max upper limit is 596, and the min upper limit is 596/8=71. If the messages in the buffer area exceed the min upper limit, the subsequent messages will be randomly dropped.

Table 9-2 Configure WRED

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map type traffic-class tc1	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 1	Set traffic priority 1
Switch(config-cmap-)# exit	Exit configuration mode
Switch(config)# policy-map type traffic-class tc	Create policy-map and enter its configuration mode
Switch(config-pmap-tc)# class type traffic-class tc1	Make association with class-map
Switch(config-pmap-tc-c)# random-detect maximum-threshold 596	Configure upper packet drop limit as 596
Switch(config-pmap-tc-c)# exit	Exit configuration mode
Switch(config-pmap-tc)# exit	Exit to global configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# service-policy type traffic-class tc	Apply QoS policy
Switch(config-if)# end	Exit global configuration mode
Switch# show qos interface eth-0-1 egress	Show QoS configurations

Configuration Verification

Switch# show qos interface eth-0-1 egress

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Max-Queue-Limit(Cell)	ECN
0	0	-	-	dynamic	level 0	-
1	0	-	-	random-drop	596	Disable
2	0	-	-	dynamic	level 0	-
3	0	-	-	tail-drop	2000	2000
4	0	-	-	dynamic	level 0	-
5	0	-	-	dynamic	level 0	-
6	0	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

Schedule

Messages at different classes are scheduled by strict priority (SP); messages at the same class are scheduled by WDRR.

The example below shows how to map queues to different classes and configure the weight for WDRR scheduling.

- configure terminal
- Create class-map priority, and specify the priority;
- Create policy-map priority, and make association with the class-map previously defined;
- Specify the scheduling priority of the corresponding traffic priority in policy-map priority mode;
- Specify the bandwidth of the corresponding traffic priority in policy-map priority mode;
- Interface IFNAME enters the interface matching corresponding policy table. IFNAME is the interface name.

The example below shows how to configure egress queue scheduling parameters. The priority of flows numbered 5 and 6 is the highest (6), and that of flow numbered 2 is 2, and the bandwidth is 20% of link bandwidth.

Table 9-3 Configure Scheduling

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map type traffic-class tc5	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 5	Set traffic priority 5
Switch(config-cmap-)# exit	Exit the configuration mode
Switch(config)# class-map type traffic-class tc6	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 6	Set traffic priority 6
Switch(config-cmap-)# exit	Exit the configuration mode
Switch(config)# class-map type traffic-class tc2	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 2	Set traffic priority 2
Switch(config-cmap-)# exit	Exit the configuration mode
Switch(config)# policy-map type traffic-class tc	Create policy-map and enter its configuration mode
Switch(config-pmap-tc)# class type traffic-class tc5	Make association with class-map tc5
Switch(config-pmap-tc-c)# priority level 6	Set priority level as 6
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# class type traffic-class tc6	Make association with class-map tc6

Switch(config-pmap-tc-c)# priority level 6	Set priority level as 6
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# class type traffic-class tc2	Make association with class-map tc2
Switch(config-pmap-tc-c)# bandwidth percentage 20	Specify the bandwidth as 20% of link bandwidth
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# exit	Exit the configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# service-policy type traffic-class tc	Apply QoS policy
Switch(config-if)# end	Exit global configuration mode
Switch# show qos interface eth-0-1 egress	Show QoS configuration

Configuration Verification

Switch# show qos interface eth-0-1 egress

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Max-Queue-Limit(Cell)	ECN
0	0	-	-	dynamic	level 0	-
1	0	-	-	random-drop	596	Disable
2	0	20	-	dynamic	level 0	-
3	0	-	-	tail-drop	2000	2000
4	0	-	-	dynamic	level 0	-
5	6	-	-	dynamic	level 0	-
6	6	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

Port Policing

All flows passing through physical interfaces of switches can be set with a guaranteed rate, and flows higher than the guaranteed rate will be discarded.

The example below shows how to configure port policer to realize the guaranteed rate.

- configure terminal
- Interface IFNAME enters the interface matching corresponding policy table. IFNAME is the interface name.
- port-policer input|output color-blind|color-aware cir <8- 100000000 > cbs <1000-640000> ebs <1000-640000>| eir <8-100000000> ebs <1000-640000> drop-color exceed|violate can be set with port policer.

Use the “no port-policier input|output” command to delete port-policer configuration.

The example below shows steps of configuring ingress port policer, where packet discard will be performed if the average rate of received packets exceeds 48000-kbps.

Table 9-4 Configure port policing

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop	Set guaranteed rate of the port as 48000kbps
Switch(config-if)# end	Exit to privilege mode
Switch# show qos interface eth-0-1 statistics policer port input	Show QoS configuration status

Configuration Verification

Switch# show qos interface eth-0-1 statistics policer port input

```
Interface: eth-0-1
 input port policer:
  color blind
   CIR 48000 kbps, CBS 10000 bytes, EBS 20000 bytes
   drop violate packets
```

I. Shaping

Interface Shaping

All flows passing through physical interfaces of switches can be shaped, and flows higher than the shaping rate will be cached. If the cache is exhausted, the subsequent messages will be discarded until the cache is purged.

The example below shows how to configure physical-interface-based traffic shaping.

- configure terminal
- Interface IFNAME enters the interface matching corresponding policy table. IFNAME is the interface name.
- qos shape rate <0-100000000> is used to specify thresholds of port traffic shaping.

The “No shape” command is used to delete traffic shaping configuration.

The example below shows the process of configuring traffic shaping. The received traffic will be discarded if its rate exceeds 1000Mbps.

Table 9-5 Configure port traffic shaping

Switch#configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# qos shape rate 1000000	Configure to discard port traffic if its rate exceeds 1000Mbps
Switch(config-if)# end	Exit to privilege mode
Switch# show running-config interface eth-0-1	Show QoS configuration status

Configuration Verification

Switch# show running-config interface eth-0-1

```
Building configuration...
!
interface eth-0-1
 service-policy type traffic-class tc
 qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop
 qos shape rate 1000000
!
```

Queue Shaping

Flows can be shaped when passing through the queues in the egress direction of switches, and flows higher than the shaping rate will be cached. If the cache is exhausted, the following messages will be discarded until the cache is purged.

The example below shows how to configure traffic shaping on egress queues

- configure terminal
- Create class-map priority, and specify the priority;
- Create policy-map priority, and make association with the class-map previously defined;
- Specify the traffic shaping of the corresponding traffic priority in policy-map priority mode;
- Interface IFNAME enters the interface matching the corresponding policy table. IFNAME is the interface name.

The “No shape rate” command is used to delete queue shaping

The example shows how to configure queue shaping for queue 3. Messages will be discarded if the traffic rate in queue 3 exceeds 1000Mbps.

Table 9-6 Configure queue traffic shaping in the egress direction

Switch# configure terminal	Enter global configuration mode
Switch(config)# class-map type traffic-class tc3	Create class-map and enter its configuration mode
Switch(config-cmap-tc)# match traffic-class 3	Configure traffic priority as 3
Switch(config-cmap-)# exit	Exit configuration mode
Switch(config)# policy-map type traffic-class tc	Create policy-map and enter its configuration mode
Switch(config-pmap-tc)# class type traffic-class tc3	Make association with class-map
Switch(config-pmap-tc-c)# shape rate 1000000	Perform queue shaping at the rate of 1000Mbps
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# exit	Exit to configuration mode
Switch(config)# interface eth-0-1	Enter port configuration mode
Switch(config-if)# service-policy type traffic-class tc	Apply QoS policies
Switch(config-if)# end	Exit global configuration mode
Switch# show qos interface eth-0-1 egress	Show QoS configuration

Configuration Verification

Switch# show qos interface eth-0-1 egress

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Max-Queue-Limit(Cell)	ECN
0	0	-	-	dynamic	level 0	-
1	0	-	-	random-drop	596	Disable
2	0	20	-	dynamic	level 0	-
3	0	-	1000000	tail-drop	2000	2000
4	0	-	-	dynamic	level 0	-
5	6	-	-	dynamic	level 0	-
6	6	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

I. Policy

The steps of deploying QoS policies are as below.

- Identify and differentiate traffic classes.
- Configure policies for different traffic classes.
- Apply the policies to interfaces.

Perform Traffic Classification via ACL

Perform IP traffic classification via IP ACL.

The example below shows how to establish IP ACL for traffic differentiation and classification.

- configure terminal
- Use the “ip access-list ACCESS-LIST-NAME” command to create ACL, wherein ACCESS-LIST-NAME is ACL name.
- Establish one or more ACEs following the ACL User Configuration Guide.

NOTE

Use the “no ip access-list” command to delete access list configuration.

The example shows how to permit host access of three IP address classes, wherein the component of the network address corresponding to host is wildcard. If the host IP address is out the match range of the list, the host access will be denied.

Table 9-7 Configure Traffic Policy

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip access-list ip-acl	Enter IP ACL configuration mode
Switch(config-ip-acl)# permit any 128.88.12.0 0.0.0.255 any	Permit traffic with source IP adress 128.88.12.x
Switch(config-ip-acl)# permit any 28.88.0.0 0.0.255.255 any	Permit traffic with source IP address 28.88.x.x
Switch(config-ip-acl)# permit any 11.0.0.0 0.255.255.255 any	Permit traffic with source IP address 11.xx.x.x
Switch(config-ip-acl)# end	Exit to privilege mode
Switch# show access-list ip ip-acl	Show ACL configuration status

Configuration Verification

Switch# show access-list ip ip-acl

```
ip access-list ip-acl
 10 permit any 128.88.12.0 0.0.0.255 any
 20 permit any 28.88.0.0 0.0.255.255 any
 30 permit any 11.0.0.0 0.255.255.255 any
```

Establish Classification Mapping Table

The example below shows how to perform IP traffic classification of specific interfaces in accordance with the classification table. The process involves establishing classification mapping table and matching rules.

- configure terminal
- Use the “ip access-list ACCESS-LIST-NAME” command to create ACL, wherein ACCESS-LIST-NAME is ACL name.
- Establish one or more ACEs as needed. Please see the ACL User Configuration Guide for steps.
- Use the “class-map (match-any|match-all) NAME” command to create a classification mapping table. Match-any refers to matching by OR logic, namely performing classification as long as one entry of the table is matched. Match-all refers to matching by AND logic, namely performing classification only if all entries of the table are matched. NAME is the classification mapping table name.

By default, match-any is applied.

- Use the “match access-group NAME” command to define the standard of classification, wherein NAME is the name of the ACL table to be associated.

Use the “no class-map” command to delete the configuration of classification mapping table.

The example shows how to create a classification mapping table named cmap1 with IP access list to permit any traffic from the source host to the destination host.

Table 9-8 Establish A Classification Mapping Table

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip access-list ip-acl	Enter IP ACL configuration mode.
Switch(config-ip-acl)# permit any any any	Permit any packet
Switch(config-ip-acl)# quit	Exit to global configuration mode
Switch(config)# class-map cmap1	Create cmap1, and enter classification mapping table configuration mode
Switch (config-cmap)# match access-group ip-acl	Add ip-acl into cmap1
Switch (config-cmap)# quit	Exit to privilege mode
Switch# show class-map cmap1	Show classification table configuration

Configuration Verification

Switch# show class-map cmap1

```
CLASS-MAP-NAME: cmap1 (match-any)
  match access-group: ip-acl
```

Create Policy Table

The example below shows how to create a policy table for traffic classification, marking and control.

- configure terminal
- Use the “ip access-list” command to create an IP ACL.
- Use the “class-map type qos NAME” command to create a classification mapping table.
- Use the “policy-map type qos NAME” command to create a policy table, wherein NAME is the name of the policy table.
- Use the “class NAME” command to define a traffic classification entry, wherein NAME is the name of the entry.
- Use the “set traffic-class <1-6>” command to set message priority for matching the traffic classification table.
- Use the “set color red|yellow|green” command to set message color for matching the traffic classification table.
- Use the “policer color-blind|color-aware cir <8-10000000> cbs <1000-640000> ebs <1000-640000>| eir <8-10000000> ebs <1000-128000> (exceed | violate) drop” command to define a policy.
- exit
- exit
- Interface IFNAME enters the interface matching corresponding policy table, wherein IFNAME is the interface name.
- Use the “service-policy type qos input NAME” to apply the policy table to ingress and egress traffic of the interface.

Only one policy mapping table is allowed in each direction under the interface.

Use the “no policy-map” command to delete an existing policy table; use the “no set priority color” command to remove priority color; use the “no policer” command to delete an existing policer; use the “no service-policy input|output” command to delete the configuration of policy table on an interface.

The example shows how to create and apply a policy table to ingress traffic of an interface. The configured IP ACL permits traffic from 10.1.00 address, and the traffic will be discarded once its average rate exceeds 48000-kbps.

Table 9-9 Create Policy Table

Switch#configure terminal	Enter global configuration mode
Switch(config)# ip access-list ip-acl	Enter IP ACL configuration mode
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	Permit traffic with source IP address 10.1.x.x
Switch(config-ip-acl)# quit	Exit to global configuration mode

Switch(config)# class-map type qos cmap1	Create cmap1, and enter classification mapping table configuration mode
Switch (config-cmap)# match access-group ip-acl	Add ip-acl into cmap1
Switch (config-cmap)# quit	Exit to global configuration mode
Switch(config)# policy-map type qos pmap1	Configure pmap1, and enter policy-map configuration mode
Switch(config-pmap)# class type qos cmap1	Add cmap1 into pmap1
Switch(config-pmap-c)# policer color-blind cir 48000 cbs 10000 ebs 16000 violate drop	Set guaranteed rate of the port as 48000kbps
Switch(config-pmap-c)# exit	Exit to policy map configuration mode
Switch(config-pmap)# quit	Exit to global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# service-policy type qos input pmap1	Apply pmap1 to interface
Switch(config-if)# end	Exit to privilege mode
Switch# show policy-map pmap1	Show policy table configuration.

Configuration Verification

Switch# show policy-map pmap1

```
POLICY-MAP-NAME: pmap1 ( type qos)
  State: attached
  CLASS-MAP-NAME: cmap1
   match access-group: ip-acl
     policer color-blind cir 48000 cbs 10000 ebs 16000 violate drop
```

Create Aggregation Policy

The example below shows how to create an aggregation policy table for traffic classification, marking and control.

- configure terminal
- Use the “qos aggregate-policer NAME color-blind|color-aware cir <0-100000000> cbs <0-640000> ebs <0- 640000>| eir <0-100000000> ebs <0-640000> exceed|violate drop” command to specify the parameters of an aggregation policy to which multiple traffic classification policies contained in one or more policy tables are required to apply.
- Use the “class-map type qos NAME” command to create a classification mapping table.
- Use the “policy-map type qos NAME” command to create a policy table.

- Use the “class type qos NAME” command to define a traffic classification entry.
- Use the “aggregate-policer NAME” command to apply an aggregation policy of traffic classification policies contained in one or more policy tables.
- exit
- exit
- Use the “interface IFNAME” command to enter the interface matching corresponding policy table.
- Use the “service-policy type qos input NAME” to apply the policy table to ingress and egress traffic of the interface.

NOTE

Only one policy mapping table is allowed in each direction under the interface.

Use the “no policer-aggregate” command to delete an aggregate policy from the policy table; use the “no qos aggregate-policer” command to delete an aggregate policy.

The example shows how to create and apply an aggregate policy to multiple entries of the policy table. As shown in the example, “IP ACLs” command permits traffic from network address 10.1.0.0 and host address 11.3.1.1, and the average rate has been configured. If the average traffic rate exceeds 48000-kbps and the traffic rate exceeds 8000-byte, the traffic will be discarded. The policy table is applied to ingress traffic of the interface.

Table 9-10 Create Aggregation Policy

Switch#configure terminal	Enter global configuration mode
Switch(config)# ip access-list ip-acl1	Enter IP ACL configuration mode
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	Permit traffic with source IP address 10.1.x.x
Switch(config-ip-acl)# exit	Exit to global configuration mode
Switch(config)# ip access-list ip-acl2	Enter IP ACL configuration mode
Switch(config-ip-acl)# permit any host 11.3.1.1 any	Permit traffic from source IP address 11.3.1.1
Switch(config-ip-acl)# exit	Exit to global configuration mode
Switch(config)# qos aggregate-policer transmit1 color-blind cir 48000 cbs 8000 ebs 10000 violate drop	Configure the guaranteed rate of the aggregate policier as 48000kbps
Switch(config)# class-map type qos cmap1	Create cmap1, and enter classification mapping table configuration mode
Switch(config-cmap)# match access-group ip-acl1	Add ip- acl1 into cmap1
Switch(config-cmap)# exit	Exit to global configuration mode
Switch(config)# class-map type qos cmap2	Create cmap1, and enter classification mapping table configuration mode

Switch(config-cmap)# match access-group ip-acl2	Add ip- acl1 into cmap1
Switch(config-cmap)# exit	Exit to global configuration mode
Switch(config)# policy-map type qos aggflow1	Configure pmap1, and enter policy-map configuration mode
Switch(config-pmap)# class type qos cmap1	Add cmap1 into pmap1
Switch(config-pmap-c)# aggregate-policer transmit1	Set cmap1 as aggregate policer transmit1
Switch(config-pmap-c)# exit	Exit to policy map configuration mode
Switch(config-pmap)# class type qos cmap2	Add cmap1 into pmap1
Switch(config-pmap-c)# aggregate-policer transmit1	Set cmap1 as aggregate policer transmit1
Switch(config-pmap-c)# exit	Exit to policy map configuration mode
Switch(config-pmap)# exit	Exit to global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# service-policy type qos input aggflow1	Apply aggregate policer aggflow1 to the interface
Switch(config-if)# exit	Exit to interface configuration mode
Switch(config)# exit	Exit to global configuration mode
Switch# show qos aggregate-policer	Show aggregate policer configuration state

Configuration Verification

Switch# show qos aggregate-policer

```
Aggreate policer: transmit1
 color blind
 CIR 48000 kbps, CBS 8000 bytes, EBS 10000 bytes
 drop violate packets
```

10 IPv6 Security Configuration Guide

10.1 DHCPv6 Snooping Configuration

10.1.1 Introduction

DHCPv6 Snooping is a security feature like firewall action between untrusted DHCPv6 client and trusted DHCPv6 server. DHCPv6 Snooping executes the following actions:

- Validating DHCPv6 messages are from an untrusted source and filtering out invalid messages.
- Establishing and maintaining DHCPv6 Snooping binding databases, which contain the IPv6 address information rented by DHCPv6 clients.
- The DHCPv6 Snooping feature is realized in software, and all DHCPv6 messages are intercepted in chip and directly sent to the CPU for processing.

10.1.2 Topology

Error! Not found reference source. To test the network topology of DHCPv6 snooping, two PCs and one switch are needed to construct the testing environment, as shown below.

- Computer A acts as DHCPv6 server
- Computer B acts as DHCPv6 client
- Switch acts as DHCPv6 snooping

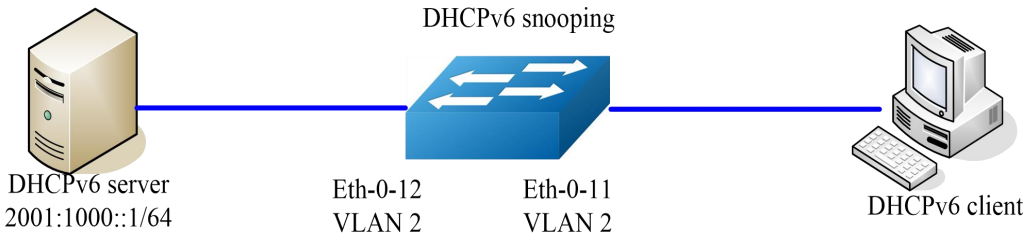


Figure 10-2 DHCP v6 Topological Graph

10.1.3 Configuration

Configure VLAN

Switch# configure terminal	Enter global configuration mode
Switch(config)# vlan database	Configure VLAN database
Switch(config-vlan)# vlan 2	Create VLAN 2
Switch(config-vlan)# exit	Exit to global configuration mode

Configure Interface eth-0-12

Switch(config)# interface eth-0-12	Enter interface configuration mode
Switch(config-if)# switchport	Set as switch port
Switch(config-if)# switchport access vlan 2	Add interface into VLAN 2
Switch(config-if)# dhcpv6 snooping trust	Configure the interface as trust
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface configuration mode

Configure Interface eth-0-11

Switch(config)# interface eth-0-11	Enter interface configuration mode
Switch(config-if)# switchport	Set as switch port
Switch(config-if)# switchport access vlan 2	Add interface into VLAN 2
Switch(config-if)# no shutdown	Enable the interface

Switch(config-if)# exit	Exit global configuration mode

Enable DHCPv6 Snooping Global Feature

Switch(config)# service dhcpv6 enable	Enable dhcp service
Switch(config)# dhcpv6 snooping	Enable dhcp snooping feature
Switch(config)# dhcpv6 snooping vlan 2	Enable dhcp snooping feature on VLAN 12

10.1.4 Command Validation

Step 1 The steps of checking the interface configuration for validity are as below.

Switch# show running-config interface eth-0-12

```
!
interface eth-0-12
switchport access vlan 2
dhcpv6 snooping trust
!
```

Switch# show running-config interface eth-0-11

```
!
interface eth-0-11
 switchport access vlan 2
!
```

Step 2 Use the following commands to check DHCPv6 service status.

Switch# show services

```
Networking services configuration:
Service Name        Status
============================================================
dhcp                disable
dhcpv6              enable
```

Step 3 Use the following command to print dhcpv6 snooping configuration and check the current configuration.

Switch# show dhcpv6 snooping config

```
dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 2
```

Step 4 Use the following command to check dhcpv6 snooping statistics.

Switch# show dhcpv6 snooping statistics

```
DHCPv6 snooping statistics:
```

```
=======================================================
DHCPv6 packets                  21
Packets forwarded               21
Packets invalid                 0
Packets dropped                 0
```

Step 5 Use the following command to display dhcpv6 snooping binding information.

Switch# show dhcpv6 snooping binding all

```
DHCPv6 snooping binding table:
VLAN MAC Address    Lease(s)    Interface   IPv6 Address
=======================================================
2    0016.76a1.7ed9 978         eth-0-11    2001:1000::2
```

11 IPv6 Route Configuration Guide

11.1 IPv6 Unicast Route Configuration

11.1.1 Introduction

Static routing is a special route that is manually configured by administrators. In the case of simple network structure, configuring a static route is enough for normal operation of network. Rationally setting and using a static route helps improving network performance and guaranteeing bandwidth for important network applications. Static route has a defect as follows: in the case of network malfunction or topological changes, the route might become unreachable, to result in network interruption. In such case, network administer manually changing the static routing configuration is required.

This example demonstrates how to enable a static route in a simple network topological structure. Static routing is of great use in small networks. Static routing can provide a simple solution to make several destinations reachable. For large networks, dynamic routing protocol applies. A static route consists of a network prefix (host address) and a next hop (gateway).

11.1.2 Topology

Figure 11-1 Static IPv6 Routing Topology

11.1.3 Configure Static IPv6 Route

I. Switch1 Configuration

Switch1# configure terminal	Enter global configuration mode
Switch1 (config)# ipv6 enable	Enable IPv6
Switch1(config)# interface eth-0-9	Enter interface mode

Switch1 (config-if)# no switchport	Set the interface as layer3 interface
Switch1(config-if)# no shutdown	Open the interface
Switch1 (config-if)# ipv6 address auto link-local	Automatically generate link-local address
Switch1 (config-if)# ipv6 address 2001:1::1/64	Configure global unicast address
Switch1(config-if)# exit	Exit interface mode
Switch1 (config)# ipv6 route 2001:2::/64 2001:1::2	Configure IPv6 static route
Switch1 (config)# end	Exit global configuration mode

II. Switch2 configuration

Switch2# configure terminal	Enter global configuration mode
Switch2 (config)# ipv6 enable	Enable IPv6
Switch2(config)# interface eth-0-9	Enter interface mode
Switch2 (config-if)# no switchport	Set the interface as layer3 interface
Switch2(config-if)# no shutdown	Open the interface
Switch2 (config-if)# ipv6 address auto link-local	Automatically generate link-local address
Switch2 (config-if)# ipv6 address 2001:1::2/64	Configure global unicast address
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-17	Enter interface mode
Switch2 (config-if)# no switchport	Set the interface as layer3 interface
Switch2(config-if)# no shutdown	Open the interface
Switch2 (config-if)# ipv6 address auto link-local	Automatically generate link-local address
Switch2 (config-if)# ipv6 address 2001:2::2/64	Configure global unicast address
Switch2(config-if)# exit	Exit interface mode
Switch2 (config)# end	Exit global configuration mode

III. Switch2 configuration

Switch3# configure terminal	Enter global configuration mode
Switch3 (config)# ipv6 enable	Enable IPv6
Switch3(config)# interface eth-0-17	Enter interface mode
Switch3 (config-if)# no switchport	Set the interface as layer3 interface
Switch3(config-if)# no shutdown	Open the interface
Switch3 (config-if)# ipv6 address auto link-local	Automatically generate link-local address
Switch3 (config-if)# ipv6 address 2001:2::3/64	Configure global unicast address
Switch3(config-if)# exit	Exit interface mode
Switch3 (config)# ipv6 route 2001:1::/64 2001:2::2	Configure IPv6 static route
Switch3 (config)# end	Exit global configuration mode

11.1.4 Command Validation

Switch1# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
C      2001:1::/64
       via ::, eth-0-9, 02:08:50
C      2001:1::1/128
       via ::1, eth-0-9, 02:08:50
S      2001:2::/64 [1/0]
       via 2001:1::2, eth-0-9, 02:05:36
C      fe80::/10
       via ::, Null0, 02:09:11
```

Switch2# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
C      2001:1::/64
       via ::, eth-0-9, 12:03:37 AM
C      2001:1::2/128
       via ::1, eth-0-9, 12:03:37 AM
C      2001:2::/64
       via ::, eth-0-17, 12:03:21 AM
C      2001:2::2/128
```

```
    via ::1, eth-0-17, 12:03:21 AM
C       fe80::/10
    via ::, Null0, 12:03:44 AM
```

Switch3# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
    [*] - [AD/Metric]
Timers: Uptime
S       2001:1::/64 [1/0]
    via 2001:2::2, eth-0-17, 12:02:14 AM
C       2001:2::/64
    via ::, eth-0-17, 12:03:28 AM
C       2001:2::3/128
    via ::1, eth-0-17, 12:03:28 AM
C       fe80::/10
    via ::, Null0, 12:03:53 AM
```

Ping Switch3 on Switch1:

Switch1# ping ipv6 2001:2::3

```
PING 2001:2::3(2001:2::3) 56 data bytes
64 bytes from 2001:2::3: icmp_seq=0 ttl=63 time=127 ms
64 bytes from 2001:2::3: icmp_seq=1 ttl=63 time=132 ms
64 bytes from 2001:2::3: icmp_seq=2 ttl=63 time=124 ms
64 bytes from 2001:2::3: icmp_seq=3 ttl=63 time=137 ms
64 bytes from 2001:2::3: icmp_seq=4 ttl=63 time=141 ms
--- 2001:2::3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 124.950/132.719/141.251/5.923 ms, pipe 2
```

11.2 Dot1x Configuration

11.2.1 Introduction

OSPF (open shortest path first) is a link-state-based interior gateway protocol developed by IETF organization. Short for OSPF version 3, OSPFv3 mainly supports IPv6 route in accordance with RFC5340 (OSPF for IPv6, OSPFv3 and OSPFv2 share many things in common:

- Router ID, Area ID and LSA Link State ID are still 32-bit.
- Protocol message type: Hello message, DD message, LSR message, LSU message and LSAck message.
- Neighbor discovery and adjacency establishing mechanism
- LSA flooding and aging mechanism.

The differences between OSPFv3 and OSPFv2 include:

- OSPFv3 is link-based, while OSPFv2 is network-based.
- In OSPFv3, multiple instances can run on one link.

- The topological relation of OSPFv3 is separate from IPv6 prefix information.
- Link-local address is taken as a route next-hop
- Link lsa and link-local flooding range is increased

The current system supports the following OSPFv3 features:

- **Supporting stub area:** Support routing redistribution, including importing the routes learned from other routing protocols into OSPFv3 or the routes learned from OSPFv3 into other routing protocols.
- Supporting OSPFv3 multi-process.
- Supporting link multi-instance.

11.2.2 References

OSPF module is based on the following RFC:

RFC 5340 – OSPF for IPv6

11.2.3 Configure Basic OSPFv3

Create an OSPFv3 process on the router on which OSPFv3 is to be enabled first, and manually specify the OSPFv3 Router ID The configuration is as below.

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# end	Go back to configuration mode
Switch# show ipv6 protocols	Check the configured protocols

Delete OSPFv3 process with command “no router ipv6 ospf *process-id*” in global mode.

11.2.4 Enable OSPF

This example shows the minimum configuration for enabling OSPFv3 on an interface.

I. Topology

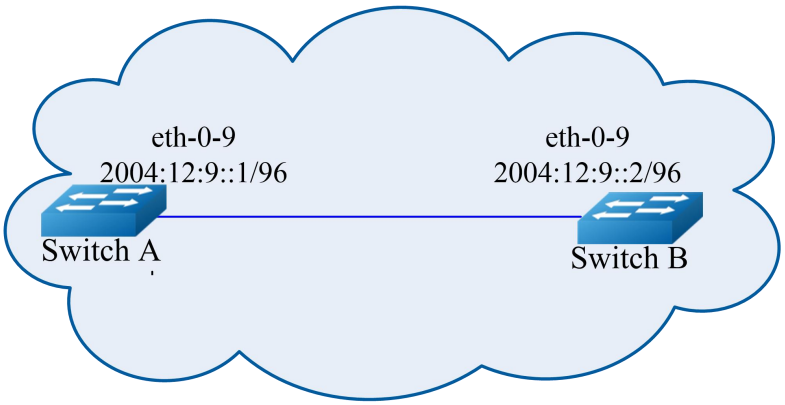


Figure 11-2 OSPFv3 Autonomous System

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# exit	Exit tunnel1 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 200	Create OSPFv3 process id as 200

Switch(config-router)# router-id 2.2.2.2	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode

III. Command validation

Use the following commands to validate the configurations above:

show ipv6 ospf database

show ipv6 ospf interface

show ipv6 ospf neighbor

show ipv6 ospf route

Switch A

Switch# show ipv6 ospf database

```
        OSPFv3 Router with ID (1.1.1.1) (Process 100)
            Link-LSA (Interface eth-0-9)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.9         1.1.1.1         614 0x80000001 0x6a40     1
0.0.0.9         2.2.2.2          68 0x80000001 0x4316     1
            Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum   Link
0.0.0.0         1.1.1.1          54 0x80000003 0xb74b     1
0.0.0.0         2.2.2.2          55 0x80000003 0x9965     1
            Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.9         1.1.1.1          54 0x80000001 0x3ed1
            I ntra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.2         1.1.1.1          53 0x80000001 0x450a     1  Network-LSA
```

Switch# show ipv6 ospf neighbor

```
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/Backup     00:00:33    eth-0-9    0
```

Switch# show ipv6 ospf route

```
OSPFv3 Process (100)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
  Destination                              Metric
    Next-hop
C  2004:12:9::/96                             1
    directly connected, eth-0-9, Area 0.0.0.0
```

Switch B

Switch# show ipv6 ospf database

```
          OSPFv3 Router with ID (2.2.2.2) (Process 200)
              Link-LSA (Interface eth-0-9)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.9         1.1.1.1         774 0x80000001 0x6a40     1
0.0.0.9         2.2.2.2         228 0x80000001 0x4316     1
              Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum   Link
0.0.0.0         1.1.1.1         217 0x80000003 0xb74b     1
0.0.0.0         2.2.2.2         214 0x80000003 0x9965     1
              Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.9         1.1.1.1         215 0x80000001 0x3ed1
              Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.2         1.1.1.1         214 0x80000001 0x450a     1  Network-LSA
```

Switch# show ipv6 ospf neighbor

```
OSPFv3 Process (200)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/DR         00:00:35    eth-0-9    0
```

Switch# show ipv6 ospf route

```
OSPFv3 Process (200)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
          E1 - OSPF external type 1, E2 - OSPF external type 2
  Destination                              Metric
    Next-hop
C  2004:12:9::/96                               1
    directly connected, eth-0-9, Area 0.0.0.0
```

11.2.5 Configure Priority

This example mainly shows how to configure interface priority. The interface of high priority becomes DR. Interfaces of 0 priority cannot be elected for DR. The priority of Switch C is 0, higher than the default priority (1) of Switch A and Switch B, so Switch C becomes the DR of the network.

I. Topology

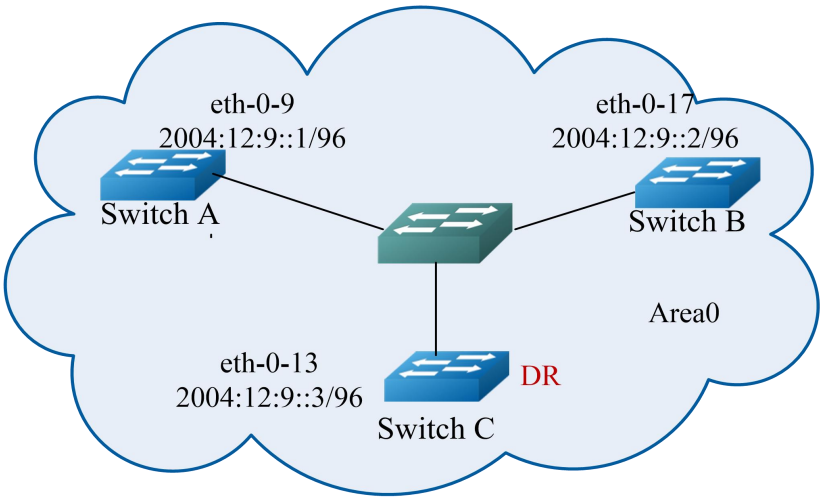


Figure 11-3 OSPFv3 Priority

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 200	Create OSPFv3 process id as 200
Switch(config-router)# router-id 2.2.2.2	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 300	Create OSPFv3 process id as 300
Switch(config-router)# router-id 3.3.3.3	Specify Router ID
Switch(config-router)# exit	Exit OPSFv3 configuration mode
Switch(config)# interface eth-0-13	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::3/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode

III. Command validation

Use the following commands to validate the configurations above:

show ipv6 ospf neighbor

show ipv6 ospf interface

Switch C

Switch# show ipv6 ospf interface

```
eth-0-13 is up, line protocol is up
  Interface ID 13
  IPv6 Prefixes
    fe80::ee66:91ff:fe45:db00/10 (Link-Local Address)
    2004:12:9::3/96
  OSPFv3 Process (300), Area 0.0.0.0, Instance ID 0
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 10
    Designated Router (ID) 3.3.3.3
      Interface Address fe80::ee66:91ff:fe45:db00
    Backup Designated Router (ID) 2.2.2.2
      Interface Address fe80::c629:f2ff:fe02:3600
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 12:00:01 AM
        Neighbor Count is 2, Adjacent neighbor count is 2
```

Switch# show ipv6 ospf neighbor

```
OSPFv3 Process (300)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/DROther      00:00:32    eth-0-13   0
2.2.2.2           1   Full/Backup       00:00:36    eth-0-13   0
```

11.2.6 Configure OSPFv3 Area Parameters

You can configure several OSPFv3 area parameters selectively. The areas are configured as a stub via the parameters. Stub area refers to specific areas, the ABR of Stub area doesn't spread the autonomous system external routes they receive, and the routing table size and the quantity of routing information passing of routers in such areas will largely decrease. To make sure that the routes outwards the autonomous system are still reachable, the ABR in this area will generate a default route and release it to other non-ABR routers in Stub area.

Route aggregation refers to ABR or ASBR aggregating routing information with the same prefix and sending one route to other areas only. After AS is partitioned into different areas, route aggregation can be utilized to reduce routing information and the size of routing table between the areas to increase the operating rate of routers. If the network numbers are consecutive, you can use the "area range" command to aggregate the consecutive network segments into one segment. By this, ABR will send an aggregated LSA only, and any other LSA within the aggregation network segment specified via this command will not be sent out separately, which can reduce LSDB size in other areas.

I. Topology

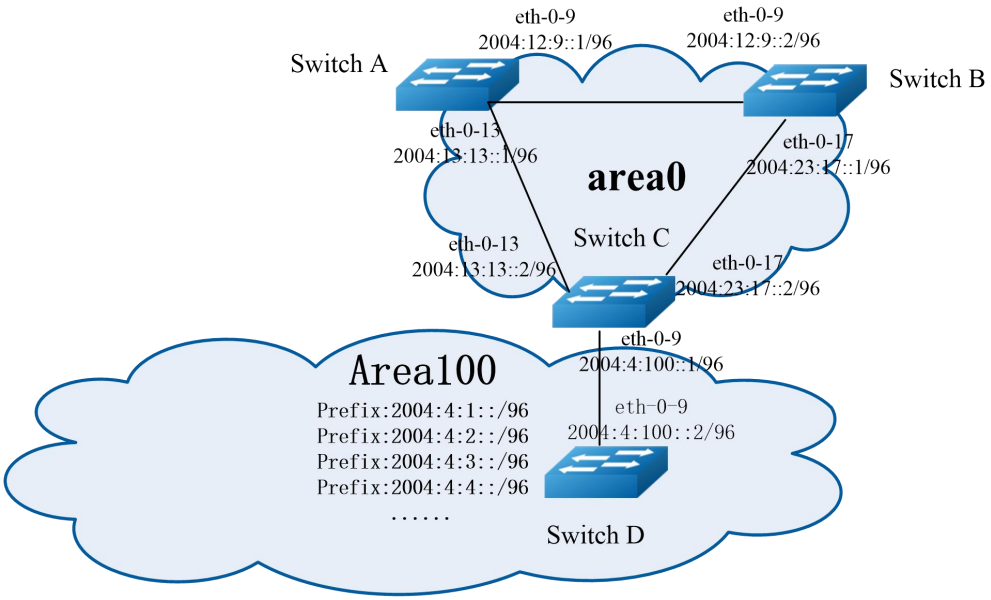


Figure 11-4 OSPFv3 Area

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:13:13::2/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 200	Create OSPFv3 process id as 200
Switch(config-router)# router-id 2.2.2.2	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:11:17 PM::1/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 300	Create OSPFv3 process id as 300
Switch(config-router)# router-id 3.3.3.3	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-13	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:13:13::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:11:17 PM::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:100::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.

Switch(config)# router ipv6 ospf 300	Enter OSPF process id 300
Switch(config-router)# area 100 range 2004:4::/32	Assign a prefix to distribute to OSPFv3 area 0
Switch(config-router)# area 100 stub no-summary	Set area 100 as stub area
Switch(config-if)# end	Exit configuration mode

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 400	Create OSPFv3 process id as 400
Switch(config-router)# router-id 4.4.4.4	Specify Router ID
Switch(config-router)# area 100 stub no-summary	Set area 100 as stub area
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:100::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:1::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-2	Enter interface mode

Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:2::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-3	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:3::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-4	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:4::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	Add the interface into OSPFv3 process300, area100, instance0
Switch(config-if)# end	Exit configuration mode

III. Command validation

Use the "**show ipv6 route**" command to validate the configurations above.

Switch A

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
```

```
Timers: Uptime
O IA    2004:4::/32 [110/3]
        via fe80::c629:f2ff:fe02:3600, eth-0-13, 00:01:00
C       2004:12:9::/96
        via ::, eth-0-9, 12:15:56 AM
C       2004:12:9::1/128
        via ::1, eth-0-9, 12:15:56 AM
C       2004:13:13::/96
        via ::, eth-0-13, 12:15:55 AM
C       2004:13:13::2/128
        via ::1, eth-0-13, 12:15:55 AM
O       2004:23:17::/96 [110/2]
        via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:08:10
        via fe80::c629:f2ff:fe02:3600, eth-0-13, 12:08:10 AM
C       fe80::/10
        via ::, Null0, 12:15:57 AM
```

Switch B

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O IA    2004:4::/32 [110/3]
    via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:00:57 AM
C       2004:12:9::/96
    via ::, eth-0-9, 12:12:24 AM
C       2004:12:9::2/128
    via ::1, eth-0-9, 12:12:24 AM
O       2004:1:13 PM::/96 [110/2]
    via fe80::b242:55ff:fe05:ff00, eth-0-9, 00:07:52
    via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:07:52 AM
C       2004:11:17 PM::/96
    via ::, eth-0-17, 12:12:24 AM
C       2004:11:17 PM::1/128
    via ::1, eth-0-17, 12:12:24 AM
C       fe80::/10
    via ::, Null0, 12:12:26 AM
```

Switch C

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        Dr - DHCPV6 Relay
        [*] - [AD/Metric]
Timers: Uptime
O       2004:4::/32 [110/0]
     via ::, Null0, 00:08:31
O       2004:4:1::/96 [110/2]
     via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:01:08 AM
O       2004:4:2::/96 [110/2]
     via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:01:08 AM
O       2004:4:3::/96 [110/2]
     via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:01:08 AM
O       2004:4:4::/96 [110/2]
     via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:01:08 AM
C       2004:4:100::/96
     via ::, eth-0-9, 00:08:32
C       2004:4:100::1/128
     via ::1, eth-0-9, 12:08:32 AM
O       2004:12:9::/96 [110/2]
     via fe80::b242:55ff:fe05:ff00, eth-0-13, 12:08:03 AM
     via fe80::bc22:aeff:fe64:aa00, eth-0-17, 12:08:03 AM
O       2004:1:13 PM::/96 [110/1]
     via fe80::b242:55ff:fe05:ff00, eth-0-13, 12:08:18 AM
C       2004:11:17 PM::/96
     via ::, eth-0-17, 00:08:32
C       2004:11:17 PM::2/128
     via ::1, eth-0-17, 12:08:32 AM
C       fe80::/10
     via ::, Null0, 12:08:34 AM
```

Switch D

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        Dr - DHCPV6 Relay
        [*] - [AD/Metric]
Timers: Uptime
O IA    ::/0 [110/2]
     via fe80::c629:f2ff:fe02:3600, eth-0-9, 12:00:53 AM
C       2004:4:1::/96
     via ::, eth-0-1, 12:03:09 AM
C       2004:4:1::1/128
     via ::1, eth-0-1, 12:03:09 AM
C       2004:4:2::/96
     via ::, eth-0-2, 12:03:08 AM
C       2004:4:2::1/128
     via ::1, eth-0-2, 12:03:08 AM
C       2004:4:3::/96
```

```
    via ::, eth-0-3, 12:03:08 AM
C   2004:4:3::1/128
    via ::1, eth-0-3, 12:03:08 AM
C   2004:4:4::/96
    via ::, eth-0-4, 12:03:09 AM
C   2004:4:4::1/128
    via ::1, eth-0-4, 12:03:09 AM
C   2004:4:100::/96
    via ::, eth-0-9, 12:03:09 AM
C   2004:4:100::2/128
    via ::1, eth-0-9, 12:03:09 AM
C   fe80::/10
    via ::, Null0, 12:03:10 AM
```

11.2.7 Configure OSPF Redistribution Route

Intra-area and inter-area routings describe the network structure inside AS, while external routing describes how to choose routing for reaching destination addresses other than AS. OSPF classifies the introduced AS external routing into Type1 and Type2.

Type1 refers to routes IGP (accepting interior gateway protocol), such as static route and RIPng route. Since this type is of high credibility and is comparable to OSPFv3's routes in respect of cost, so the cost for reaching Type1 is equal to the sum of the cost from this router to corresponding ASBR and of that from the ASBR to this routing destination address.

Type2 refers to routes accepting EGP (exterior gateway protocol). Since this type is of low credibility, so OSPFv3 protocols regard the cost from ASBR towards autonomous system is much higher than the cost for reaching ASBR within the autonomous system. Thus, the former will be primarily considered first, that's the cost for reaching Type2 is equal to the cost from ASBR to the routing destination address. If two routes with equal cost are calculated out, the cost from the router to corresponding ASBR can be considered. In the example below, RIP route will be redistributed into OSPFv3 network as an external route.

I. Topology

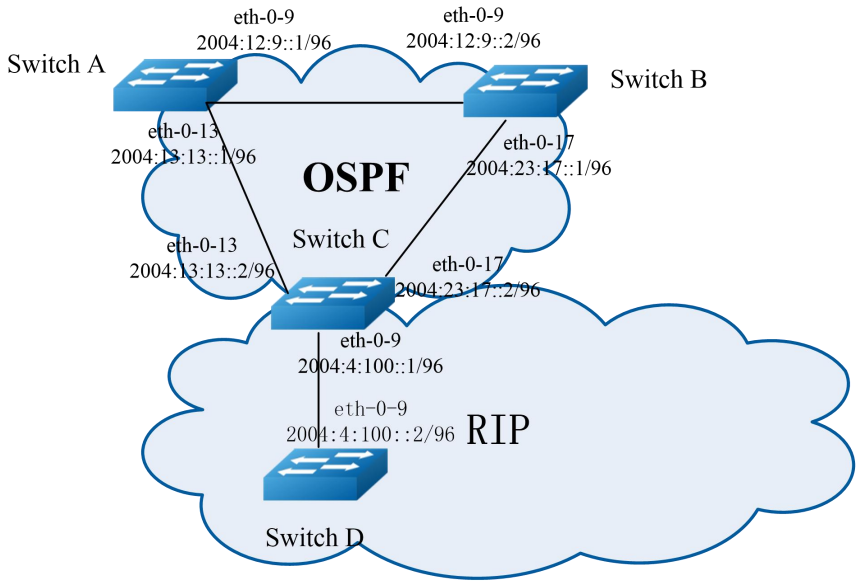


Figure 11-5 OSPFv3 Route Redistribution

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-13	Enter interface mode

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:13:13::2/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 200	Create OSPFv3 process id as 200
Switch(config-router)# router-id 2.2.2.2	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:11:17 PM::1/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 300	Create OSPFv3 process id 300
Switch(config-router)# router-id 3.3.3.3	Specify Router ID
Switch(config-router)# redistribute ripng	Redistribute ripng to OSPE
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-13	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:13:13::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:11:17 PM::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)# router ipv6 rip	Enable ripng
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:100::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Add the interface into RIPng routing domain

Switch(config-if)# end	Exit configuration mode

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 rip	Enable ripng
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:100::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Add the interface into RIPng routing domain
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:4:1::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Add the interface into RIPng routing domain
Switch(config-if)# end	Exit configuration mode

III. Command validation

Use the following commands to validate the configurations above:

show ipv6 ospf database external

show ipv6 route

Switch A

Switch# show ipv6 route

IPv6 Routing Table

```
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O E2   2004:4:1::/96 [110/20]
    via fe80::c629:f2ff:fe02:3600, eth-0-13, 12:00:03 AM
C      2004:12:9::/96
    via ::, eth-0-9, 12:34:20 AM
C      2004:12:9::1/128
    via ::1, eth-0-9, 12:34:20 AM
C      2004:1:13 PM::/96
    via ::, eth-0-13, 12:34:19 AM
C      2004:1:13 PM::2/128
    via ::1, eth-0-13, 12:34:19 AM
O      2004:11:17 PM::/96 [110/2]
    via fe80::bc22:aeff:fe64:aa00, eth-0-9, 12:26:34 AM
    via fe80::c629:f2ff:fe02:3600, eth-0-13, 12:26:34 AM
C      fe80::/10
    via ::, Null0, 12:34:21 AM
```

Switch# show ipv6 ospf database external

```
        OSPFv3 Router with ID (1.1.1.1) (Process 100)
            AS-external-LSA
 LS age: 140
 LS Type: AS-External-LSA
 Link State ID: 0.0.0.1
 Advertising Router: 3.3.3.3
 LS Seq Number: 0x80000001
 Checksum: 0x66F7
 Length: 44
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2004:4:1::/96
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0
```

Switch B

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O E2   2004:4:1::/96 [110/20]
    via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:02:43 AM
```

```
C       2004:12:9::/96
        via ::, eth-0-9, 12:33:31 AM
C       2004:12:9::2/128
        via ::1, eth-0-9, 12:33:31 AM
O       2004:1:13 PM::/96 [110/2]
        via fe80::b242:55ff:fe05:ff00, eth-0-9, 12:28:59 AM
        via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:28:59 AM
C       2004:11:17 PM::/96
        via ::, eth-0-17, 12:33:31 AM
C       2004:11:17 PM::1/128
        via ::1, eth-0-17, 12:33:31 AM
C       fe80::/10
        via ::, Null0, 12:33:33 AM
```

Switch# show ipv6 ospf database external

```
show ipv6 ospf database external
        OSPFv3 Router with ID (2.2.2.2) (Process 200)
            AS-external-LSA
 LS age: 195
 LS Type: AS-External-LSA
 Link State ID: 0.0.0.1
 Advertising Router: 3.3.3.3
 LS Seq Number: 0x80000001
 Checksum: 0x66F7
 Length: 44
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2004:4:1::/96
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0
```

Switch C

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
R       2004:4:1::/96 [120/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:03:43 AM
C       2004:4:100::/96
        via ::, eth-0-9, 12:07:01 AM
C       2004:4:100::1/128
        via ::1, eth-0-9, 12:07:01 AM
O       2004:12:9::/96 [110/2]
        via fe80::b242:55ff:fe05:ff00, eth-0-13, 12:29:57 AM
        via fe80::bc22:aeff:fe64:aa00, eth-0-17, 12:29:57 AM
O       2004:1:13 PM::/96 [110/1]
```

```
    via fe80::b242:55ff:fe05:ff00, eth-0-13, 12:30:12 AM
C       2004:11:17 PM::/96
    via ::, eth-0-17, 12:30:26 AM
C       2004:11:17 PM::2/128
    via ::1, eth-0-17, 12:30:26 AM
C       fe80::/10
    via ::, Null0, 12:30:28 AM
```

Switch# show ipv6 ospf database external

```
show ipv6 ospf database external
        OSPFv3 Router with ID (3.3.3.3) (Process 300)
            AS-external-LSA
 LS age: 250
 LS Type: AS-External-LSA
 Link State ID: 0.0.0.1
 Advertising Router: 3.3.3.3
 LS Seq Number: 0x80000001
 Checksum: 0x66F7
 Length: 44
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2004:4:1::/96
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0
```

Switch D

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
C       2004:4:1::/96
    via ::, eth-0-1, 12:04:48 AM
C       2004:4:1::1/128
    via ::1, eth-0-1, 12:04:48 AM
C       2004:4:100::/96
    via ::, eth-0-9, 12:06:59 AM
C       2004:4:100::2/128
    via ::1, eth-0-9, 12:06:59 AM
C       fe80::/10
    via ::, Null0, 12:07:00 AM
```

11.2.8 Configure OSPFv3 Cost

You can set an optimal routing by modifying interface COST value. As shown in the example below, Switch B is made into the next hop of Switch A by modifying the COST value.

The default interface COST value is 1 (1000M speed). Eth-0-17 priority of Switch B is 100, and eth-0-9 priority of Switch D is 150. Then, the Cost of reaching Switch C 2004:3:1::/96 will be different:

Switch B: 1+1+100 = 102

Switch C: 1+1+150 = 152

I. Topology

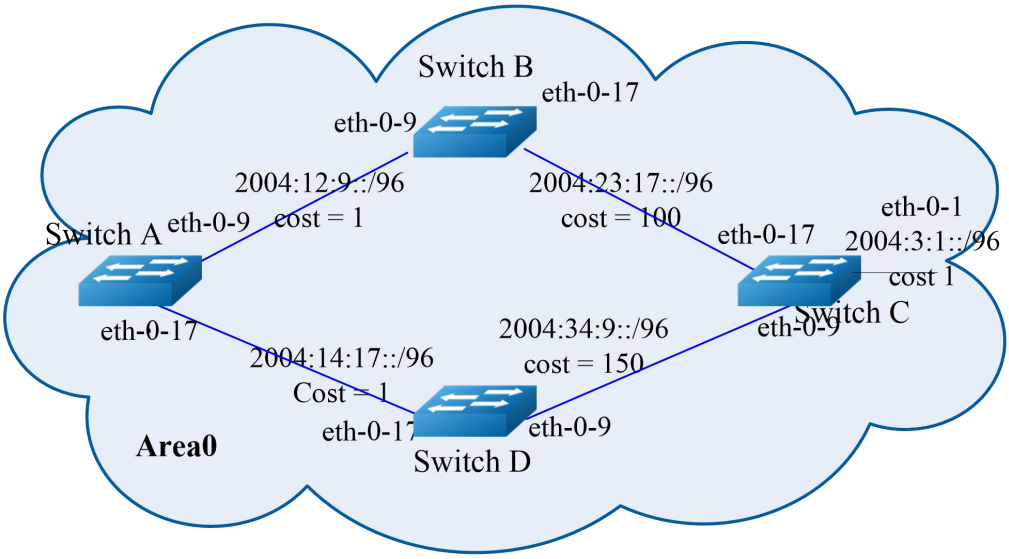


Figure 11-6 OSPFv3 Cost

II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 100	Create OSPFv3 process id as 100
Switch(config-router)# router-id 1.1.1.1	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::1/96	Configure IPv6 address

Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:2:17 PM::1/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	Add the interface into OSPFv3 process100, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 200	Create OSPFv3 process id as 200
Switch(config-router)# router-id 2.2.2.2	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:12:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# end	Exit configuration mode
Switch# configure terminal	Enter configuration mode.
Switch(config)#interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# no shutdown	Up interface

Switch(config-if)# ipv6 address 2004:11:17 PM::1/96	Configure interface IP address
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	Add the interface into OSPFv3 process200, area0, instance0
Switch(config-if)# ipv6 ospf cost 100	Configure OSPFv3 interface cost
Switch(config-if)# end	Exit configuration mode

Switch C

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 300	Create OSPFv3 process id as 300
Switch(config-router)# router-id 3.3.3.3	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:11:17 PM::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:34:9::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface

Switch(config-if)# ipv6 address 2004:3:1::1/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode

Switch D

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# router ipv6 ospf 400	Create OSPFv3 process id as 400
Switch(config-router)# router-id 4.4.4.4	Specify Router ID
Switch(config-router)# exit	Exit OSPFv3 configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:34:9::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# ipv6 ospf cost 150	Configure OSPFv3 interface cost
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-17	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2004:2:17 PM::2/96	Configure IPv6 address
Switch(config-if)# ipv6 router ospf 400 area 0 instance 0	Add the interface into OSPFv3 process300, area0, instance0
Switch(config-if)# end	Exit configuration mode

III. Command validation

Use the "**show ipv6 ospf route**" command to validate the configurations above.

Switch A

Switch# show ipv6 ospf route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O      2004:3:1::/96 [110/102]
    via fe80::bc22:aeff:fe64:aa00, eth-0-9, 12:08:06 AM
C      2004:12:9::/96
    via ::, eth-0-9, 1:15:43 AM
C      2004:12:9::1/128
    via ::1, eth-0-9, 1:15:43 AM
C      2004:2:17 PM::/96
    via ::, eth-0-17, 12:18:38 AM
C      2004:2:17 PM::1/128
    via ::1, eth-0-17, 12:18:38 AM
O      2004:11:17 PM::/96 [110/101]
    via fe80::bc22:aeff:fe64:aa00, eth-0-9, 12:08:06 AM
O      2004:34:9::/96 [110/102]
    via fe80::bc22:aeff:fe64:aa00, eth-0-9, 12:03:56 AM
C      fe80::/10
    via ::, Null0, 1:15:44 AM
```

Switch B

Switch# show ipv6 ospf route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O      2004:3:1::/96 [110/101]
    via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:08:33 AM
C      2004:12:9::/96
    via ::, eth-0-9, 1:12:40 AM
C      2004:12:9::2/128
    via ::1, eth-0-9, 1:12:40 AM
O      2004:2:17 PM::/96 [110/2]
    via fe80::b242:55ff:fe05:ff00, eth-0-9, 12:18:43 AM
C      2004:11:17 PM::/96
    via ::, eth-0-17, 1:12:40 AM
C      2004:11:17 PM::1/128
    via ::1, eth-0-17, 1:12:40 AM
```

```
O       2004:34:9::/96 [110/101]
        via fe80::c629:f2ff:fe02:3600, eth-0-17, 12:04:23 AM
C       fe80::/10
        via ::, Null0, 1:12:42 AM
```

Switch C

Switch# show ipv6 ospf route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
C       2004:3:1::/96
        via ::, eth-0-1, 12:13:54 AM
C       2004:3:1::1/128
        via ::1, eth-0-1, 12:13:54 AM
O       2004:12:9::/96 [110/2]
        via fe80::bc22:aeff:fe64:aa00, eth-0-17, 12:19:47 AM
O       2004:2:17 PM::/96 [110/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 12:02:27 AM
C       2004:11:17 PM::/96
        via ::, eth-0-17, 1:09:02 AM
C       2004:11:17 PM::2/128
        via ::1, eth-0-17, 1:09:02 AM
C       2004:34:9::/96
        via ::, eth-0-9, 12:04:52 AM
C       2004:34:9::1/128
        via ::1, eth-0-9, 12:04:52 AM
C       fe80::/10
        via ::, Null0, 1:09:04 AM
```

Switch D

Switch# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O       2004:3:1::/96 [110/103]
        via fe80::b242:55ff:fe05:ff00, eth-0-17, 12:02:35 AM
O       2004:12:9::/96 [110/2]
        via fe80::b242:55ff:fe05:ff00, eth-0-17, 12:02:35 AM
C       2004:2:17 PM::/96
```

```
    via ::, eth-0-17, 12:04:09 AM
C   2004:2:17 PM::2/128
    via ::1, eth-0-17, 12:04:09 AM
O   2004:11:17 PM::/96 [110/102]
    via fe80::b242:55ff:fe05:ff00, eth-0-17, 12:02:35 AM
C   2004:34:9::/96
    via ::, eth-0-9, 12:06:06 AM
C   2004:34:9::2/128
    via ::1, eth-0-9, 12:06:06 AM
C   fe80::/10
    via ::, Null0, 12:44:59 AM
```

11.2.9 Configure Listening OSPFv3

You can run commands to show detailed statistics, such as the content of IPv6 routing table, cache and database.

Switch# show ipv6 ospf	Show OSPF process information
Switch # show ipv6 ospf database database-summary Switch # show ipv6 ospf database router Switch # show ipv6 ospf database network self-originate Switch # show ipv6 ospf database inter-router Switch # show ipv6 ospf database intra-prefix Switch # show ipv6 ospf database inter-prefix Switch # show ipv6 ospf database link Switch # show ipv6 ospf database external	Show OSPF link status information base
Switch # show ipv6 ospf interface	Show OPSFv3 interface information
Switch # show ipv6 ospf neighbor	Show OSPFv3 neighbor information

11.3 RIPng Configuration

11.3.1 Introduction

RIPng (Routing Information Protocol Next Generation) is an extension of RIP-2 protocol of IPv4 network, and most concepts involved in the latter still apply to RIPng.

RIPng is a simple interior gateway protocol (IGP) that is mainly applied in small-scale network.

RIPng is a protocol based on distance-vector algorithm, which conducts routing information exchange via UDP message. RIPng measures the distance from the destination via hop count, which is called routing cost. In RIPng, the hop count of moving from a router to the directly connected network is 0, that of moving to the network reachable via one router is 1, and so on.

To limit the convergence time, RIP specifies cost value to be an integer between 0 and 15, and a hop count with cost value above or equal to 16 is defined as infinity, meaning unreachability of destination network or host.

To enhance the performance and prevent routing loops, RIPng supports split horizon. RIPng also can introduce routes obtained based on other routing protocols.

For application in IPv6 network, RIPng has made some modifications to the previous RIP:

- UDP port number: Use UDP port 521 to send and receive routing information.
- Multicast address: Use FF02::9 as RIPng router multicast address within the link-local range
- Next hop address: Use a 128-bit IPv6 address
- Source address: Use link-local address FE80::/10 as source destination for sending RIPng routing information update messages.

11.3.2 References

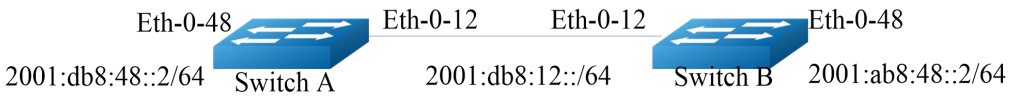
RIPng module is based on the following RFC:

RFC 2080 – RIPng for IPv6

11.3.3 Configure Enabling RIPng

The steps of enabling RIPng routing protocol on two switches are as shown in Figure 8-1

I. Topology



II. Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 rip	Enable RIPng
Switch(config-router)# exit	Exit routing mode
Switch(config)# interface eth-0-12	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2001:db8:12::1/64	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Enable RIPng on the interface
Switch(config-if)# exit	Exit interface mode

Switch(config)# interface eth-0-48	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2001:db8:48::2/64	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Enable RIPng on the interface

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 rip	Enable RIPng
Switch(config-router)# exit	Exit routing mode
Switch(config)# interface eth-0-12	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2001:db8:12::2/64	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Enable RIPng on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-48	Enter interface mode
Switch(config-if)# no switchport	Enable layer 3 interface attributes
Switch(config-if)# no shutdown	Up interface
Switch(config-if)# ipv6 address 2001:ab8:49::2/64	Configure IPv6 address
Switch(config-if)# ipv6 router rip	Enable RIPng on the interface

III. Command validation

Use the following commands to validate the configurations above:

show ipv6 rip database

show ipv6 rip interface

show ipv6 protocols rip

show ipv6 route rip

Switch A output

Switch# show ipv6 rip database

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
  Network                Next Hop                If       Met Tag Time
R  2001:ab8:49::/64      fe80::1271:d1ff:fec8:3300 eth-0-12 5   0   00:02:34
Rc 2001:db8:12::/64      ::                      eth-0-12 1   0
Rc 2001:db8:48::/64      ::                      eth-0-48 1   0
```

Switch# show ipv6 rip interface

```
eth-0-12 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:db8:12::1/64
      fe80::7e14:63ff:fe76:8900/10
eth-0-48 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:db8:48::2/64
      fe80::7e14:63ff:fe76:8900/10
```

Switch# show ipv6 protocols rip

```
Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-5 seconds, next due in 7 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing:
  Interface
    eth-0-12
    eth-0-48
  Routing for Networks:
  Number of routes (including connected): 3
  Distance: (default is 120)
```

Switch# show ipv6 route rip

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
```

```
R       2001:ab8:49::/64 [120/5]
        via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:26:05
```

Switch B

Switch# show ipv6 rip database

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
  Network              Next Hop                If      Met Tag Time
Rc 2001:ab8:49::/64    ::                      eth-0-48 1   0
Rc 2001:db8:12::/64    ::                      eth-0-12 1   0
R  2001:db8:48::/64    fe80::7e14:63ff:fe76:8900 eth-0-12 2   0   00:02:33
```

Switch# show ipv6 rip interface

```
eth-0-12 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:db8:12::2/64
      fe80::1271:d1ff:fec8:3300/10
eth-0-48 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:ab8:49::2/64
      fe80::1271:d1ff:fec8:3300/10
```

Switch# show ipv6 protocols rip

```
Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-5 seconds, next due in 13 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Outgoing routes will have 3 added to metric if on list ripng_acl
  Default redistribute metric is 1
  Redistributing:
  Interface
    eth-0-12
    eth-0-48
  Routing for Networks:
  Number of routes (including connected): 3
  Distance: (default is 120)
```

Switch# show ipv6 route rip

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        Dr - DHCPV6 Relay
        [*] - [AD/Metric]
Timers: Uptime
R       2001:db8:48::/64 [120/2]
      via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:23:31 AM
```

11.3.4 Configure Metric Parameters

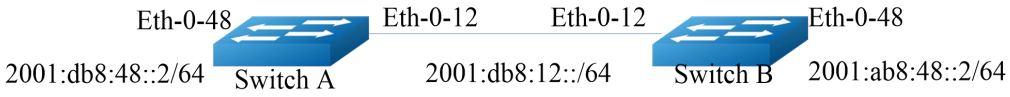
Offset metric refers to input/output metric attached to RIPng routing, including sent and received offset metric. Sending offset metric will not change the routing metric in the routing table, which will be added to the sending router only when the interface sends RIP routing information; receiving offset metric will affect the received routing metric, and the interface that receives a legal RIP route will attach the metric to the route while adding it to the routing table. Offset metric generally contains the following parameters:

- The ACL parameters for specifying adding routing metric are described as below.
  - **In**: applies to RIPng routes learned from neighboring routers
  - **Out**: applies to the RIPng notification delivered to neighboring routers
- Offset value metric matching ACL routing
- Interface with offset-list applied

  If a route matches the global offset table (not assign an interface) and an interface-based offset table, the interface-based table is prior. In such case, the metric of the interface-based is added to the route.

The example below shows how to add metric 3 to 2001:db8:48::2/64 on eth-0-12 of Switch A.

I. Topology



II. Configuration

Switch A configuration

Switch# show run

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
```

```
!
router ipv6 rip
!
```

Switch B configuration

Switch# show run

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Validation route table on Switch B

Switch# show ipv6 route rip

```
R      2001:db8:48::/64 [120/2]
       via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:44:47 AM
```

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)#ipv6 access-list ripngoffset	Create ACL.
Switch(config-ipv6-acl)# permit any 2001:db8:48::/64 any	Match corresponding network segment
Switch(config-ipv6-acl)# router ipv6 rip	Enable RIPng routing protocol
Switch(config-router)# offset-list ripngoffset out 3 eth-0-12	Set the metric value for offset list

III. Command validation

Switch B output

Switch# show ipv6 route rip

```
R      2001:db8:48::/64 [120/5]
```

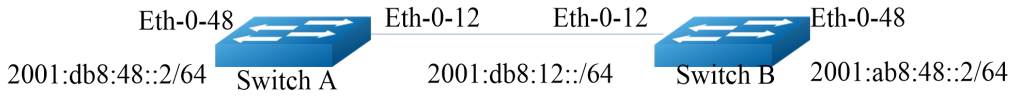
```
via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:00:07 AM
```

11.3.5 Configure Administrative Distance

By default, the administrative distance of RIPng is 120. In case of route comparison, the route with a short administrative distance stands a big chance of being selected.

The example below shows how to change RIPng administrative distance.

I. Topology



II. Configuration

Switch A configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
```

```
!
router ipv6 rip
!
```

Validation route table on Switch B

Switch# show ipv6 route rip

```
R      2001:db8:48::/64 [120/2]
       via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:44:47 AM
```

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 rip	Enable RIPng routing protocol
Switch(config-router)# distance 100	Set RIPng route administrative distance as 100

III. Command validation

Switch B output

Switch# show ipv6 route rip

```
R      2001:db8:48::/64 [100/5]
       via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:00:09 AM
```

11.3.6 Configure Redistribution

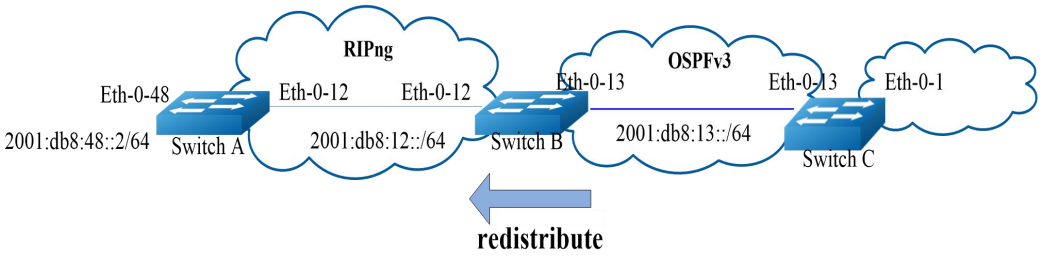
You can redistribute static routing, direct-connected routing and other routing protocols such as OSPFv3 routing to RIP, which will be sent by RIPng to its neighbors.

The default RIPng redistribution metric is 1, and the maximum is 16.

For redistributing a specific route to RIPng, the metric can be the default value or a modified value.

The example below shows how to redistribute other routing information to RIPng.

I. Topology



II. Configuration

Switch A configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-13
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:13::1/64
 ipv6 router ospf area 0
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
```

```
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
router ipv6 ospf
 router-id 1.1.1.1
```

Switch C configuration

Switch# show running-config

```
interface eth-0-1
 no switchport
   ipv6 address auto link-local
 ipv6 address 2001:db8:1::1/64
 ipv6 router ospf area 0
!
interface eth-0-13
 no switchport
 ipv6 address 2001:db8:13::2/64
 ipv6 router ospf area 0
!
router ipv6 ospf
 router-id 2.2.2.2
!
```

Validation route table on Switch A

Switch# show ipv6 route rip

```
R      2001:ab8:48::/64 [120/5]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 1:43:37 AM
```

Validation route table on Switch B

Switch# show ipv6 route

```
O      2001:db8:1::/64 [110/2]
       via fe80::5c37:1dff:febe:2d00, eth-0-13, 00:31:17
R      2001:db8:48::/64 [100/5]
       via fe80::7e14:63ff:fe76:8900, eth-0-12, 12:49:57 AM
```

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 rip	Enable RIPng routing protocol
Switch(config-router)#default-metric 2	Specify default metric
Switch(config-router)#redistribute ospfv3 metric 5	Redistribute OSPFv3 routing to RIPng

III. Command validation

Switch A output

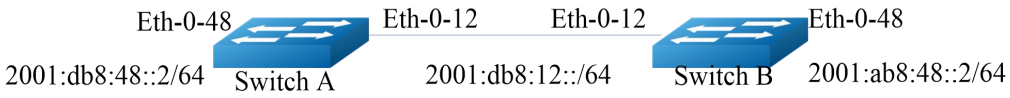
Switch# show ipv6 route rip

```
R      2001:ab8:48::/64 [120/5]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 1:48:23 AM
R      2001:db8:1::/64 [120/6]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 12:00:19 AM
```

11.3.7 Configure Split Horizon Parameters

In general, for routers connected a multicast network and using distance vector routing protocol, split horizon mechanism is applied to prevent loops. By applying the split horizon mechanism, the routes learned from an interface cannot be released out via the interface, which generally optimizes the communication between multiple routers, especially in the case of link failure. By configuring poison reverse, the routes learned from an interface can be released out via the interface, but they are unreachable because the metric value of the routes has been set as 16.

I. Topology



II. Configuration

Switch A configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B debug configuration

Switch# debug ipv6 rip packet send detail

Switch# terminal monitor

Disable Split-horizon on Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-12	Configure interface eth-0-12
Switch(config-if)# no ipv6 rip split-horizon	Disable split horizon

Oct 24 10:00:06 Switch RIPNG6-7: SEND[eth-0-12]: Send to [ff02::9]:521

Oct 24 10:00:06 Switch RIPNG6-7: SEND[eth-0-12]: RESPONSE version 1 packet size 64

Oct 24 10:00:06 Switch RIPNG6-7: 2001:ab8:49::/64 metric 4 tag 0

Oct 24 10:00:06 Switch RIPNG6-7: 2001:db8:12::/64 metric 1 tag 0

Oct 24 10:00:06 Switch RIPNG6-7: 2001:db8:48::/64 metric 5 tag 0

Enable Split-horizon on Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)#interface eth-0-12	Configure interface eth-0-12
Switch(config-if)# ipv6 rip split-horizon	Enable split horizon

Oct 24 10:05:16 AM Switch RIPNG6-7: SEND[eth-0-12]: Send to [ff02::9]:521

Oct 24 10:05:16 AM Switch RIPNG6-7: SEND[eth-0-12]: RESPONSE version 1 packet size 44

Oct 24 10:05:16 AM Switch RIPNG6-7: 2001:ab8:49::/64 metric 4 tag 0

Oct 24 10:05:16 AM Switch RIPNG6-7: 2001:db8:12::/64 metric 1 tag 0

III. Command validation

Use the following commands to validate the configurations above:

show running-config

show ipv6 rip interface

11.3.8 Configure Timer

RIPng is controlled by several timers, such as frequency of routing update, routing failure time, etc. You can adjust RIPng performance by adjusting these timers, to address your needs in Internet works better. The following parameters can be adjusted:

- Update timer defines the interval of sending update messages.
- Timeout timer defines the routing aging time. If no route update message is received within the aging time, the metric value of the route in the routing table will be set as 16.
- Garbage-Collect timer defines the period from the route metric value being changed to 16 until the route is removed from the routing table.

I. Configuration

Use the following commands to configure Timer

Switch# configure terminal	Enter configuration mode
Switch(config)# router ipv6 rip	Enable RIPng routing protocol
Switch(config-router)# timers basic 10 180 120	Specify routing table update timer as 10 seconds, routing information timeout timer 180 seconds, and garbage collect timer as 120 seconds.

II. Command validation

Use the following commands to validate the configurations above:

show running-config

show ipv6 protocols rip

Switch# show ipv6 protocols rip

```
Routing Protocol is "ripng"
 Sending updates every 10 seconds with +/-5 seconds, next due in 5 seconds
 Timeout after 180 seconds, garbage collect after 120 seconds
 Outgoing update filter list for all interface is not set
 Incoming update filter list for all interface is not set
 Outgoing routes will have 3 added to metric if on list ripng_acl
 Default redistribute metric is 2
 Redistributing:
 Interface
```

```
  eth-0-12
  eth-0-48
 Routing for Networks:
 Number of routes (including connected): 3
 Distance: (default is 100)
```

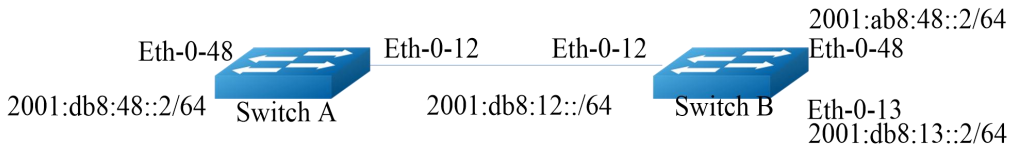
11.3.9 Configure RIPng Routing Filter List

Routers provide the function of routing information filter, with which ingress or egress filtering policy can be configured by specifying an access control list and address prefix list to filter received or released routes. A route filter list generally contains the following parameters:

- An ACL or prefix list used as filter.
- **Ingress:** The filter is applied to the learned route; **egress:** The filter is applied to the releasing route.

Interface for applying filter (optional).

I. Topology



II. Configuration

Switch A configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B configuration

Switch# show running-config

```
interface eth-0-12
 no switchport
```

```
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-13
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:13::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch A output

Switch# show ipv6 route rip

```
R      2001:ab8:48::/64 [120/5]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 12:18:29 AM
R      2001:db8:13::/64 [120/2]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 12:03:37 AM
```

Please refer to the commands below for configuring Switch B.

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 prefix-list ripngfilter seq 5 deny 2001:db8:48::/64 Switch(config)# ipv6 prefix-list ripngfilter seq 10 permit any	Establish a list
Switch(config)# router ipv6 rip	Enable RIPng routing protocol
Switch(config-router)# distribute-list prefix ripngfilter out eth-0-12	Apply policy

III. Command validation

Switch A output

Switch# show ipv6 route rip

```
R      2001:db8:13::/64 [120/2]
       via fe80::1271:d1ff:fec8:3300, eth-0-12, 12:03:37 AM
```

11.4 Ipv6 Prefix-list Configuration

11.4.1 Introduction

Routing policy is a technology of modifying routing information to change the path of network traffic, which is mainly realized by changing routing attributes (including reachability). Address prefix list is one routing policy, which can be flexibly applied. Address prefix list is identified via prefix list name. An address prefix list can contain multiple entries, each entry can individually specify a match range identified with index number in the form of network prefix. The index number indicates the order of match check. In matching process, switches checks entries identified with index number by ascending order. The matching process will end once an entry meets the conditions, and the matching of next entries will not continue.

11.4.2 Basic Configuration

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 prefix-list test seq 1 deny 2001:db8::1/32 le 48	Create address prefix list test, and create an entry numbered 1
Switch(config)# ipv6 prefix-list test permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# ipv6 prefix-list test description this ipv6 prefix list is fot test	Add address prefix list description
Switch(config)# ipv6 prefix-list test permit 2001:abc::1/32 le 48	Create an entry numbered with a default serial number
Switch(config)# exit	Exit global mode

II. Command validation

Switch# show ipv6 prefix-list detail

```
Prefix-list list number: 1
Prefix-list entry number: 3
Prefix-list with the last deletion/insertion: test
ipv6 prefix-list test:
  Description: this ipv6 prefix list is fot test
  count: 3, range entries: 0, sequences: 1 - 10
    seq 1 deny 2001:db8::1/32 le 48 (hit count: 0, refcount: 0)
    seq 5 permit any (hit count: 0, refcount: 0)
    seq 10 permit 2001:abc::1/32 le 48 (hit count: 0, refcount: 0)
```

11.4.3 Configure RIPng Simple Application

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 prefix-list aa seq 11 deny 2001:db8::1/32 le 48	Create address prefix list aa, and create an entry
Switch(config)# ipv6 prefix-list aa permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# router ipv6 rip	Enter Ripng routing mode
Switch(config-router)# distribute-list prefix aa out	Apply policy
Switch(config-router)# end	Exit Ripng routing mode

II. Command validation

Switch# show ipv6 prefix-list

```
ipv6 prefix-list aa: 2 entries
   seq 11 deny 1:db8::1/32 le 48
   seq 15 permit any
```

Switch# show running-config

```
Building configuration...
…
ipv6 prefix-list aa seq 11 deny 1:db8::1/32 le 48
ipv6 prefix-list aa seq 15 permit any
…
router ipv6 rip
distribute-list prefix aa out
```

11.4.4 Configure Route-map Simple Application

I. Configure applying ipv6 prefix-list to route-map

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 prefix-list ripng_pre_1 seq 11 permit fe80::a8f0:d8ff:fe7d:c501/128	Create an address prefix list ripng_pre_1, and create an entry
Switch(config)# ipv6 prefix-list ripng_pre_1 permit any	Create an entry to avoid being denied in the case of unmatched entry
Switch(config)# route-map ripng_rmap permit	Create route-map
Switch(config-route-map)# match ipv6 address prefix-list ripng_pre_1	Match address prefix list ripng_rmap

Switch(config-route-map)# set local-preference 200	Set actions
Switch(config-route-map)# exit	Exit routing mode
Switch(config)# router ipv6 rip	Enter Ripng routing mode
Switch(config-router)# redistribute static route-map ripng_rmap	Configure static routing redistribution
Switch(config-router)# end	Exit RIPng mode

II. Command validation

Switch # show route-map

```
route-map ripng_rmap, permit, sequence 10
  Match clauses:
    ipv6 next-hop prefix-list ripng_pre_1
  Set clauses:
    ipv6 next-hop local fe80::1
```

Switch # show running-config

```
Building configuration...
…
ipv6 prefix-list ripng_pre_1 seq 11 permit fe80::a8f0:d8ff:fe7d:c501/128
ipv6 prefix-list ripng_pre_1 seq 15 permit any
!
!
route-map ripng_rmap permit 10
 match ipv6 next-hop prefix-list ripng_pre_1
 set ipv6 next-hop local fe80::1
!

router ipv6 rip

 redistribute static route-map ripng_rmap

!

ipv6 route 2001:dbc::/64 fe80::a8f0:d8ff:fe7d:c501 eth-0-9

!
```

Switch# show ipv6 rip database

```
S  2001:dbc::/64              fe80::1                   eth-0-9  1   0
```

12 IPv6 Service Configuration Guide

12.1 IPv6 over IPv4 Tunneling Configuration

12.1.1 Introduction

Tunneling is an encapsulation technology of utilizing a network protocol to transmit another network protocol. Specifically, a network protocol encapsulates a data packet of another network protocol in its data packet and transmit it in the network. The path for transmitting encapsulated data packets in the network is called tunnel. Tunnel is a virtual point-to-point link, data packet encapsulation and de-encapsulation must be performed on the two ends of a tunnel. Tunneling refers to a whole process consisting of data encapsulating, transmitting and de-encapsulating.

Immediately after the transition from IPv4 Internet to IPv6 Internet, IPv4 Internet has been widely deployed, while IPv6 networks are still sparsely distributed in the world as island. The tunnel linking IPv4 Internet to IPv6 Internet is called IPv6 over IPv4 tunnel. IPv6 data packets are encapsulated in IPv4 data packets to realize transparent transmission of IPv6 data packets. To realize the IPv6 over IPv4 tunnel, IPv4/IPv6 dual-stack protocol must be enabled on the border switch between IPv4 and IPv6.

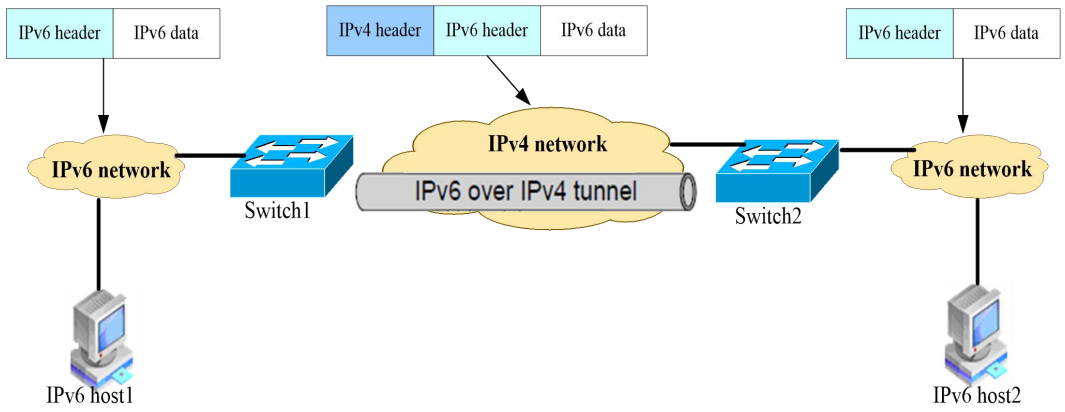


Figure 12-1: Schematic Figure of IPv6 over IPv4 Tunnel

IPv6 over IPv4 tunnel processes data packets as below:

- A device in IPv6 network sends an IPv6 message to the source device Switch 1 of the tunnel.

- Switch 1, after determining that the message must be forwarded via the tunnel based on the routing table, encapsulates the IPv6 message with an IPv4 message header and forwards it out via the physical interface of the tunnel.
- The encapsulated message passes through the tunnel and reaches the destination device Switch2, and Switch2 de-encapsulates the message after judging the message destination is a local device.
- Switch2 forwards the IPv6 message to the destination address of the de-encapsulated IPv6 message. If Switch2 exactly is the destination, it forwards the message to an upper layer protocol for processing.

  The advantage of this technology is that it is not needed to upgrade all devices to dual-stack, and only the edge devices of IPv4/IPv6 network are required to enable dual-stack and tunneling features. None of the nodes other than edge nodes needs to support dual-stack protocol. This helps making the best of the existing IPv4 network investment.

By the way of capturing IPv4 address of tunnel terminals, tunnels are classified into “configured tunnel” and “automatic tunnel”.

- If the terminal addresses of an IPv6 over IPv4 tunnel cannot be automatically captured from the destination address of IPv6 message, and must be manually configured, such a tunnel is called “configured tunnel”.
- If the terminal address of an IPv6 over IPv4 tunnel is a special IPv6 address embedded in IPv4 address, and the IPv4 addresses of the tunnel terminals can be automatically captured from the destination address of IPv6 message, such a tunnel is called “automatic tunnel”.

  The commonly used IPv6 over IPv4 tunnel modes include:

  - Configured IPv6 over IPv4 tunnel
  - 6to4 tunnel
  - ISATAP tunnel

I. Configured IPv6 over IPv4 tunnel

The source and destination addresses of configured IPv6 tunnel are manually specified, and the tunnel provides point-to-point connection. Configured IPv6 tunnel can be constructed between two border routers to provide stable connection for IPv6 networks separated by IPv4, or between the terminal system and border router to provide the terminal system with access to IPv6 networks. The head-ends of the tunnel must support IPv6/IPv4 dual-stack. Other devices must realize single protocol stack only.

Configured IPv6 tunnel requires to manually configure the source and destination addresses of the tunnel on devices. If it is to construct configured tunnels between one border device and multiple devices, it is required to configure multiple tunnels on the device. Therefore, configured tunnel is generally used between two border routers to provide access for two IPv6 networks.

II. 6to4 tunnel

- Ordinary 6to4 tunnel

  6to4 tunnel refers to point-to-multipoint automatic tunnel, and it is mainly used to connecting multiple IPv6 islands to IPv6 networks via IPv4 network. 6to4 tunnel automatically captures the IPv4 address of the tunnel terminal by embedding an IPv4 address into the destination address of IPv6 message.

6to4 tunnel adopts a special IPv6 address format, namely 6to4 address, of which the format is:

2002:IPv4 address:subnet ID:Interface ID

6to4 address has a 48-bit prefix of 2002:IPv4 address. The IPv4 address is a unique IPv4 address applied for IPv6 islands globally. The IPv4 address must be configured on the IPv6/IPv4 border switch and the physical port linking to IPv4 network. The subnet is 16-bit, and the interface ID is 64-bit, both of which are assigned by users in IPv6 island.

- 6to4 relay

  6to4 tunnel can be used for communication between 6to4 networks prefixed with 2002::/16, but IPv6 network addresses like 2002::/16 also will be adopted in IPv6 network. To realize communication between 6to4 networks and other IPv6 networks, a 6to4 router must be provided as a gateway for forwarding messages to IPv6 networks. This router is called 6to4 relay router. (If the destination address of an IP6 message is not a 6to4 address, but the next hop is a 6to4 address, then an IPv4 address will be taken from the next hop address as the destination address of tunnel.)

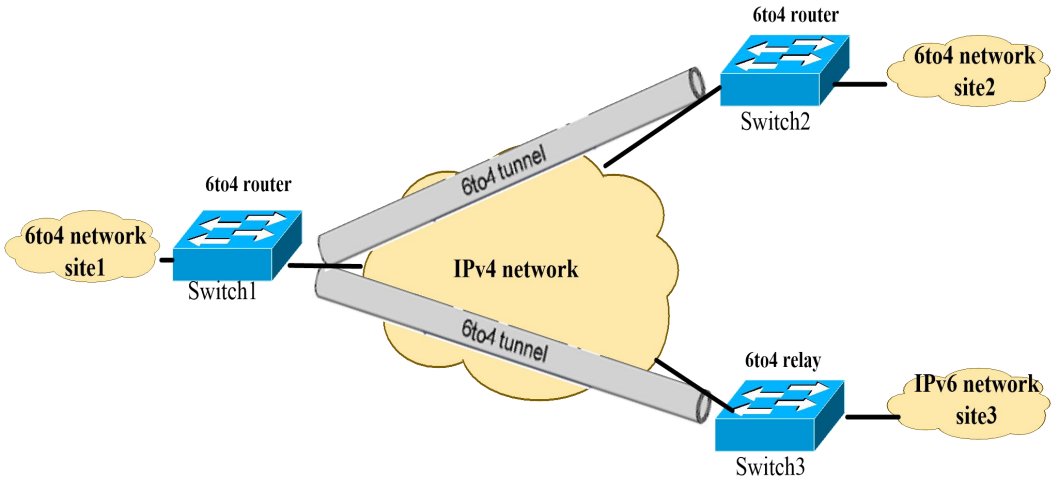


Figure 12-2: Schematic Figure of 6to4 Tunnel

As shown in the figure above, the IPv6 message searches the forwarding table based on the IPv6 destination address of the message after reaching the border router. If the egress interface is a virtual interface of an automatic 6to4 tunnel, and the destination address of the message or the next hop is a 6to4 address, an IPv4 address will be taken from the 6to4 address as destination address of the tunnel message. The source address of the tunnel message is specified on the tunnel interface.

III. ISATAP tunneling

With the popularization of IPv6 technology, more and more IPv6 hosts will be applied in the existing IPv4 networks, and ISATAP tunneling provides a good solution to this application. ISATAP tunneling is a point-to-multipoint automatic tunneling technology, by which tunnel terminals can be automatically captured by embedding an IPv4 address into the destination address of IPv6 message.

If ISATAP tunneling is applied, the destination address of IPv6 message and the IPv6 address of tunnel interface both must be of special ISATAP address format.

Prefix(64bit)::5EFE:IPv4-Address

Since the IPv4/IPv6 host and ISATAP switch are in the same IPv4 network in the case of constructing ISATAP tunnel, the IPv4 address embedded in the ISATAP address can be a public or private address. ISATAP tunneling is mainly applied for IPv6 router-IPv6 router and IPv6 host-ISATAP tunneling IPv6 router connections in IPv4 network.

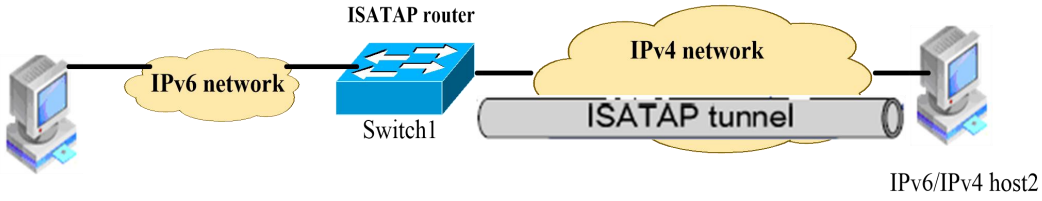


Figure 12-3: Schematic Figure of ISATAP Tunneling

As shown in the Figure above, the process of IPv4/IPv6 host capturing an IPv6 address is as below:

Step 1 IPv4/IPv6 host transmits a switch request message. IPv4/IPv6 host transmits a switch request message to ISATAP switch with a link-local address of ISATAP format, and the switch request message is encapsulated in an IPv4 message.

Step 2 ISATAP switch responds to the request. ISATAP switch responds to the switch request from the host via switch notification message. The switch notification message contains an ISATAP prefix (which is manually configured on the switch).

Step 3 IPv4/IPv6 host obtains its IPv6 address. IPv4/IPv6 host obtains its IPv6 address that combines the ISATAP prefix and 5EFE:IPv4-Address, and access the IPv6 host with this address.

12.1.2 Configure Configured Tunnel

I. Topology

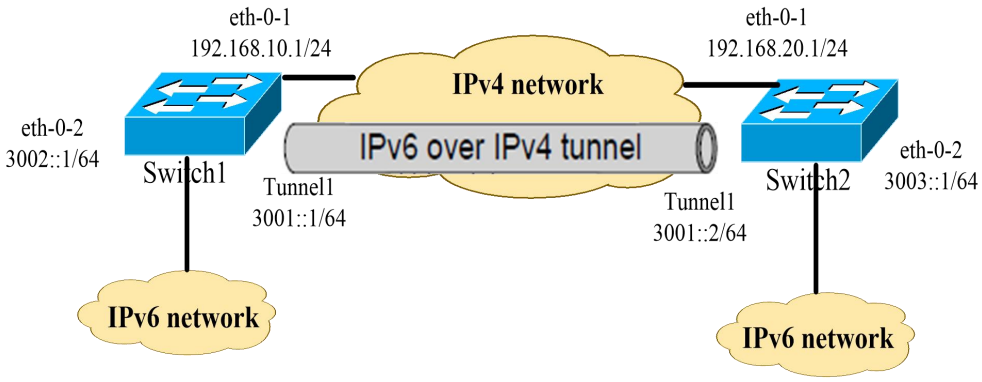


Figure 12-4: Configure Configured Tunnel

As shown in the Figure above, the two IPv6 networks are linked to the IPv4 network via Switch1 and Switch2 respectively, and it is required to

construct a configured IPv6 tunnel between Switch1 and Switch2 to make the two IPv6 networks intercommunicate with each other.

II. Configuration

Switch1

1. Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2. Configure IPv4 address, to realize layer 3 reachability of message router

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 192.168.10.1/24	Configure interface IPv4 address
Switch(config)# ip route 192.168.20.0/24 192.168.10.2	ConfigureIPv4 static route for reaching the opposite end
Switch(config)# arp 192.168.10.2 0.0.2222	Configure static ARP, 0.0.2222 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3. Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 3002::1/64	Configure interface IPv6 address

4. Configure tunnel1 Interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel destination 192.168.20.1	Configure tunnel destination
Switch(config-if)# tunnel mode ipv6ip	Configure tunnel mode as configured tunnel
Switch(config-if)# ipv6 address 3001::1/64	Configure tunnel interface IPv6 address

5. Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6. Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 3003::/16 tunnel1	Configure static routing for reaching the opposite end

Switch2

1. Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2. Configure IPv4 address, to realize layer 3 reachability of message router

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 192.168.20.1/24	Configure interface IPv4 address
Switch(config)# ip route 192.168.10.0/24 192.168.20.2	Configure static IPv4 routing for reaching the opposite end
Switch(config)# arp 192.168.20.2 0.0.1111	Configure static ARP, 0.0.1111 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3. Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 3003::1/64	Configure interface IPv6 address

4. Configure tunnel1 Interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source

Switch(config-if)# tunnel destination 192.168.10.1	Configure tunnel destination
Switch(config-if)# tunnel mode ipv6ip	Configure tunnel mode as configured tunnel
Switch(config-if)# ipv6 address 3001::2/64	Configure tunnel interface IPv6 address

5. Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6. Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 3002::/16 tunnel1	Configure static routing for reaching the opposite end

II. Check configuration result

Switch1

```
Switch1# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP, Status Valid
  Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
Switch1# show ipv6 interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::c0a8:a01
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
```

```
Hosts use stateless autoconfig for addresses.
```

Switch2

Switch1# show interface tunnel1

```
Interface tunnel1
 Interface current state: UP
 Hardware is Tunnel
 Index 8193 , Metric 1 , Encapsulation TUNNEL
 VRF binding: not bound
 Tunnel protocol/transport IPv6/IP, Status Valid
 Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
 Tunnel DSCP inherit,  Tunnel TTL 64
 Tunnel transport MTU 1480 bytes
```

Switch1# show ipv6 interface tunnel1

```
 Interface current state: UP
 The maximum transmit unit is 1480 bytes
 IPv6 is enabled, link-local address is fe80::c0a8:1401
 Global unicast address(es):
   3001::2, subnet is 3001::/64
 ICMP error messages limited to one every 1000 milliseconds
 ICMP redirects are always sent
 ND DAD is enabled, number of DAD attempts: 1
 ND router advertisement is disabled
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND router advertisements max interval: 600 secs
 ND router advertisements min interval: 198 secs
 ND router advertisements live for 1800 seconds
 ND router advertisements hop-limit is 0
 Hosts use stateless autoconfig for addresses.
```

NOTE

1. The IPv6 function must be globally enabled before configuration.
2. Settings must be made to realize layer 3 routability of IPv4 messages, otherwise tunnel message forwarding will fail.
3. Tunnel interfaces must be configured with IPv6 addresses, otherwise the router configured on the interface is inactive.

12.1.3 Configure 6to4 Tunneling

I. Topology

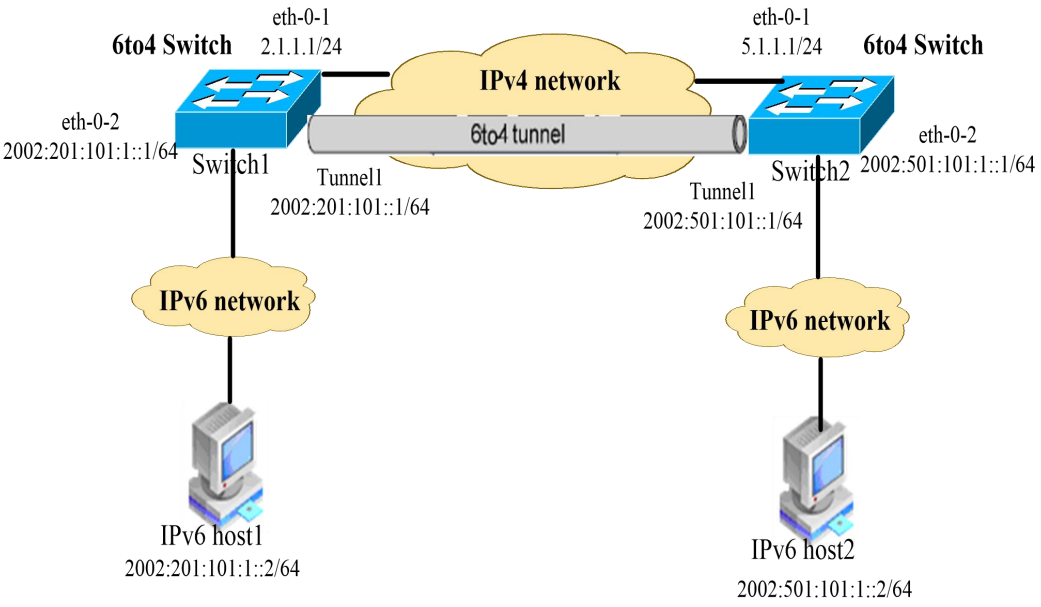


Figure 12-5: 6to4 Tunneling Configuration

As shown in the figure above, the two 6to4 networks are connected to the IPv4 network via the edge 6to4 switches (Switch1and Switch2). A 6to4 tunnel has been constructed between Switch1 and Switch2 to realize intercommunication between the hosts Host1 and Host2 in the 6to4 network.

To realize intercommunication between the 6to4 networks, the hosts of the 6to4 networks and the 6to4 router also must be configured 6to4 addresses.

- The IPv4 address of interface eth-0-1 of Switch1 is 2.1.1.1/24, which uses a 6to4 prefix of 2002:0201:0101::/48 after being converted to IPv6 address. According to subnetting of the prefix, Tunnel1 uses 2002:0201:0101::/64 subnet, and eth-0-2 uses 2002:0201:0101:1::/64 subnet.
- The IPv4 address of eth-0-1 of Switch2 is 5.1.1.1/24, which uses a 6to4 prefix of 2002:0501:0101::/48 after being converted to IPv6 address. According to subnetting of the prefix, Tunnel1 uses 2002:0501:0101::/64 subnet, and eth-0-2 uses 2002:0501:0101:1::/64 subnet.

II. Configuration

Switch1

1) Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2) Configure IPv4 address, to realize layer 3 message routability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 2.1.1.1/24	Configure interface IPv4 address
Switch(config)# ip route 5.1.1.0/24 2.1.1.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 2.1.1.2 0.0.2222	Configure static ARP, 0.0.2222 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3) Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	Configure interface IPv6 address

4) Configure tunnel interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4 tunnel
Switch(config-if)# ipv6 address 2002:201:101::1/64	Configure tunnel interface IPv6 address

5) Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6) Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode

Switch(config)# ipv6 route 2002::/16 tunnel1	Configure static routing for reaching the opposite end

Switch2

1) Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2) Configure IPv4 address, to realize layer 3 message routability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 5.1.1.1/24	Configure interface IPv4 address
Switch(config)# ip route 2.1.1.0/24 5.1.1.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 5.1.1.2 0.0.1111	Configure static ARP, 0.0.1111 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3) Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 2002:501:101:1::1/64	Configure interface IPv6 address

4) Configure tunnel interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4 tunnel
Switch(config-if)# ipv6 address 2002:501:101::1/64	Configure tunnel interface IPv6 address

5) Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6) Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 2002::/16 tunnel1	Configure static routing for reaching the opposite end

I. Check configuration result

Switch1

Switch1# show interface tunnel1

```
Interface tunnel1
 Interface current state: UP
 Hardware is Tunnel
 Index 8193 , Metric 1 , Encapsulation TUNNEL
 VRF binding: not bound
 Tunnel protocol/transport IPv6/IP 6to4, Status Valid
 Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
 Tunnel DSCP inherit,  Tunnel TTL 64
 Tunnel transport MTU 1480 bytes
```

Switch2

Switch1# show interface tunnel1

```
Interface tunnel1
 Interface current state: UP
 Hardware is Tunnel
 Index 8193 , Metric 1 , Encapsulation TUNNEL
 VRF binding: not bound
 Tunnel protocol/transport IPv6/IP 6to4, Status Valid
 Tunnel source 5.1.1.1(eth-0-1), destination UNKNOWN
 Tunnel DSCP inherit,  Tunnel TTL 64
 Tunnel transport MTU 1480 bytes
```

NOTE

1. 6To4 tunnel doesn’t have to configure destination address.
2. For automatic tunnel, tunnel ports subject to the same encapsulation protocol cannot have an identical source address.
3. Before encapsulation, if the destination IPv6 address of an IPv6 message and the IPv6 address of the tunnel interface are not in the same network segment, a forwarding route for reaching the destination IPv6 address through the tunnel interface must be configured to ensure successful forwarding of messages to be encapsulated. For automatic tunnel, users can configure static routing only and assign the egress routed port for reaching the destination IPv6 address as the tunnel interface of home terminal or a next hop as the tunnel interface address of the opposite terminal, and dynamic routing is not supported.
4. One switch allows one 6to4 tunnel only.

12.1.4 Configure 6to4 Relay

I. Topology

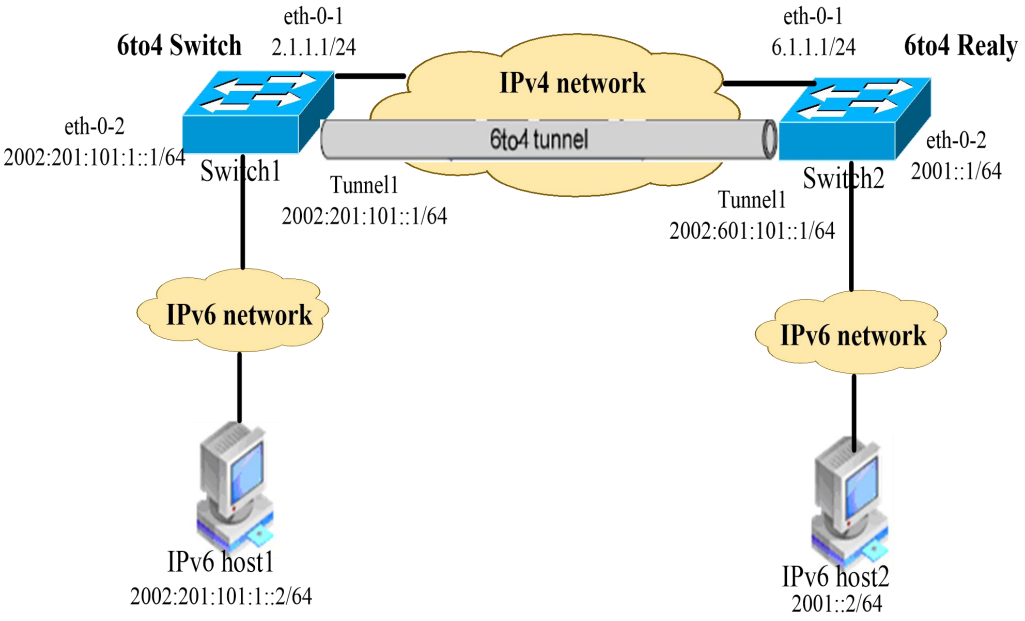


Figure 12-6: 12- 1Configure 6to4 Relay

As shown in the figure above, Switch1 acts as a 6to4 switch, and a 6to4 address is applied to the network on the IPv6 side. Switch2 acts as a 6to4 relay, and is connected to an IPv5 network (2001::/16). It is required to construct a 6to4 tunnel between Switch1 and Switch2 to realize intercommunication between the hosts Host1 and Host2 in the 6to4 network.

II. Configuration

Switch1

1) Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2) Configure IPv4 address, to realize layer 3 message routability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 2.1.1.1/24	Configure interface IPv4 address
Switch(config)# ip route 6.1.1.0/24 2.1.1.2	Configure IPv4 static routing for reaching the opposite end

Switch(config)# arp 2.1.1.2 0.0.2222	Configure static ARP, 0.0.2222 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3) Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	Configure interface IPv6 address

4) Configure tunnel Interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4 tunnel
Switch(config-if)# ipv6 address 2002:201:101::1/64	Configure tunnel interface IPv6 address

5) Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6) Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 2001::/16 2002:601:101::1	Configure static routing to IPv6-only network
Switch(config)# ipv6 route 2002:601:101::/48 tunnel1	Configure static routing to 6to4 relay

Switch2

1) Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2) Configure IPv4 address, to realize layer 3 message routability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 6.1.1.1/24	Configure interface IPv4 address
Switch(config)# ip route 2.1.1.0/24 6.1.1.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 6.1.1.2 0.0.1111	Configure static ARP, 0.0.1111 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3) Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 2001::1/64	Configure interface IPv6 address

4) Configure tunnel interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create virtual tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4 tunnel
Switch(config-if)# ipv6 address 2002:601:101::1/64	Configure tunnel interface IPv6 address

5) Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6) Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 2002::/16 tunnel1	Configure static routing for reaching the opposite end

III. Check configuration result

Switch1

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch1# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
S       2001::/16 [1/0]
        via 2002:601:101::1 (recursive via ::, tunnel1), 00:00:32
C       2002:201:101::/64
        via ::, tunnel1, 12:00:04 AM
C       2002:201:101::1/128
        via ::1, tunnel1, 00:00:04
S       2002:601:101::/48 [1/0]
        via ::, tunnel1, 12:00:22 AM
```

Switch1# show ipv6 interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::201:101
  Global unicast address(es):
    2002:201:101::1, subnet is 2002:201:101::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```

Switch2

```
Switch1# show interface tunnel1
Interface tunnel1
 Interface current state: UP
 Hardware is Tunnel
 Index 8193 , Metric 1 , Encapsulation TUNNEL
 VRF binding: not bound
 Tunnel protocol/transport IPv6/IP 6to4, Status Valid
 Tunnel source 6.1.1.1(eth-0-1), destination UNKNOWN
 Tunnel DSCP inherit,  Tunnel TTL 64
 Tunnel transport MTU 1480 bytes
```

NOTE

1. The 6to4 relay switch and 6to4 switch are configured in the same way. To realize the intercommunication between the 6to4 network and IPv6 network, however, it is needed to configure a route from the 6to4 switch to the IPv6 networks.
2. If the switch is set with a route for reaching the 6to4 relay, the tunnel mode cannot be switched.

12.1.5 Configure ISATAP Tunneling

I. Topology

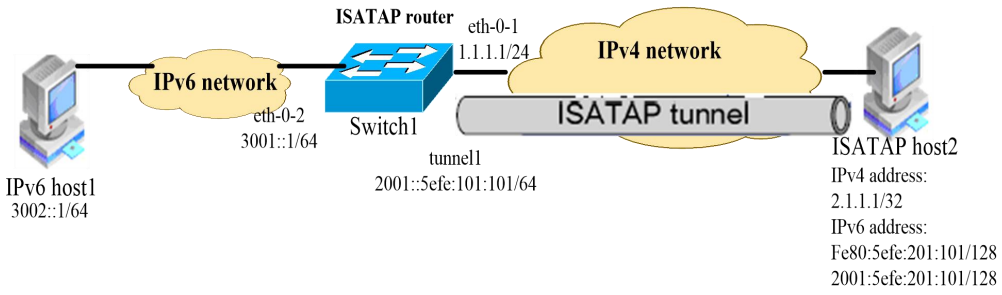


Figure 12-7: Configure ISATAP Tunneling

As shown in the figure above, the IPv6 network and the IPv4 network are connected via an ISATAP router, and the IPv6 hosts are distributed on the side of the IPv4 side. The IPv6 hosts in the IPv4 network are required to access the IPv6 network via the ISATAP tunnel.

II. Configuration

Switch1

1) Enable IPv6 function

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 enable	Globally enable IPv6

2) Configure IPv4 address, to realize layer 3 message routability

Switch# configure terminal	Enter global configuration mode

Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 1.1.1.1/24	Configure interface IPv4 address
Switch(config)# ip route 2.1.1.0/24 1.1.1.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 1.1.1.2 0.0.2222	Configure static ARP, 0.0.2222 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

3) Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ipv6 address 3001::1/64	Configure interface IPv6 address

4) Configure tunnel interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel mode ipv6ip isatap	Configure tunnel mode as ISATAP tunnel
Switch(config-if)# ipv6 address 2001::/64 eui-64	Configure tunnel interface IPv6 address
Switch(config-if)# no ipv6 nd ra suppress	Unsuppress RA message release to enable the hosts to capture some information such as address prefix from RA message released from the switch

5) Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Enable eth-0-1 as tunnel decap

6) Configure static IPv6 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ipv6 route 2001::/16 tunnel1	Configure static routing to ISATAP host

Configure ISATAP Host

The configurations on the ISATAP host depends on the operation system. The example below is for Windows XP system.

Install IPv6 protocol on the host.

C:\>ipv6 install

In Windows XP system, generally interface 2 serves as ISATAP interface, and the configurations on the host side can be completed by configuring IPv4 addresses of ISATAP switch on this interface. The details of ISATAP interface is as below:

```
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 0.0.0.0
  router link-layer address: 0.0.0.0
    preferred link-local fe80::5efe:2.1.1.1, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 25000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

C:\>ipv6 rlu 2 1.1.1.1

Running this command the host configurations can be completed. The below is still the information of ISATAP interface:

```
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 2.1.1.1
  router link-layer address: 1.1.1.1
preferred global 2001::5efe:2.1.1.1, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:2.1.1.1, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 25000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

III. Check Configuration Result

Switch1

Switch# show interface tunnel1

```
Interface tunnel1
 Interface current state: UP
 Hardware is Tunnel
 Index 8193 , Metric 1 , Encapsulation TUNNEL
 VRF binding: not bound
 Tunnel protocol/transport IPv6/IP ISATAP, Status Valid
 Tunnel source 1.1.1.1(eth-0-1), destination UNKNOWN
 Tunnel DSCP inherit,  Tunnel TTL 64
 Tunnel transport MTU 1480 bytes
```

Switch# show ipv6 interface tunnel1

```
Interface tunnel1
 Interface current state: UP
 The maximum transmit unit is 1480 bytes
 IPv6 is enabled, link-local address is fe80::101:101
 Global unicast address(es):
   2001::101:101, subnet is 2001::/64 [EUI]
 ICMP error messages limited to one every 1000 milliseconds
 ICMP redirects are always sent
 ND DAD is enabled, number of DAD attempts: 1
 ND router advertisement is enabled
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND router advertisements max interval: 600 secs
 ND router advertisements min interval: 198 secs
 ND next router advertisement due in 359 secs.
 ND router advertisements live for 1800 seconds
 ND router advertisements hop-limit is 0
 Hosts use stateless autoconfig for addresses.
```

NOTE

1. ISATAP tunnel doesn’t have to configure destination address.
2. For automatic tunnel, tunnels ports subject to the same encapsulation protocol cannot have an identical source address.
3. Before encapsulation, if the destination IPv6 address of an IPv6 message and the IPv6 address of the tunnel interface are not in the same network segment, a forwarding route for reaching the destination IPv6 address through the tunnel interface must be configured to ensure successful forwarding of messages to be encapsulated. For automatic tunnel, users can configure static routing only and assign the egress routed port for reaching the destination IPv6 address as the tunnel interface of home terminal or a next hop as the tunnel interface address of the opposite terminal, and dynamic routing is not supported.

12.2 NDP Configuration

12.2.1 Introduction

Network nodes (host and router) uses the neighbor discovery protocol (ND) for detecting link-layer addresses of direct-connected neighbors. A mechanism is provided for quickly validating a neighbor already cached in the table entries.

Hosts also can locate neighbor routers via ND.

This protocol is utilized as a keep-alive mechanism between network nodes for regularly detecting neighbor validity, neighbor link-layer address changes or neighbor failure events.

12.2.2 Topology

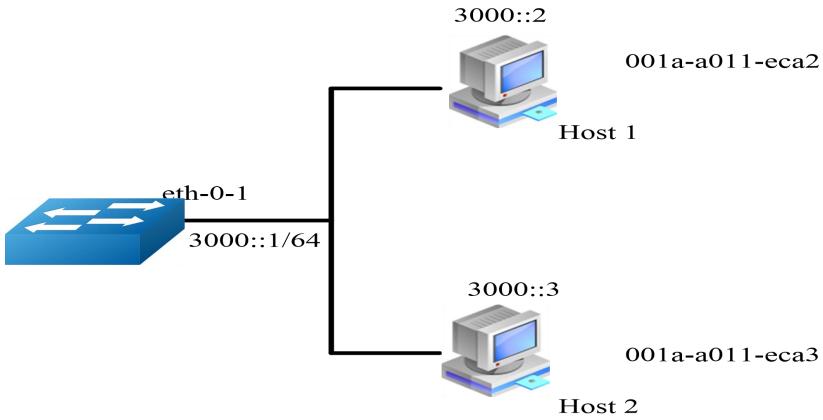


Figure 12-8: RIP Topology

12.2.3 Configuration

In this example, the address of eth-0-1 is 3000::1/64.

There are two hosts in the 3000::/64 segment, of which the addresses are 3000::2 and 3000::3 respectively, and the MAC addresses are 001a-a011-eca2 and 001a-a011-eca3 respectively. 3000::2 is configured with a static neighbor, and 3000::3 learns via dynamic protocols.

The aging time of eth-0-1 is set as 10 minutes. The NS interval is set as 2 seconds.

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure the interface as layer 3 routed port
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# ipv6 address 3000::1/64	Configure IPv6 address
Switch (config-if)# ipv6 nd reachable-time 600	Set neighbor aging time

Switch (config-if)# ipv6 nd ns-interval 2000	Set NS interval
Switch(config-if)# exit	Exit interface mode
Switch (config)# ipv6 neighbor 3000::2 001a.a011.eca2	Configure static neighbor table entries
Switch(config)# end	Exit global configuration mode.

12.2.4 Command Validation

Switch # show ipv6 neighbors

IPv6 address	Age	Link-Layer Addr	State	Interface
3000::2	-	001a-a011-eca2	REACH	eth-0-1
3000::3	6	001a-a011-eca3	REACH	eth-0-1
fe80::6d8:e8ff:fe4c:e700	6	001a-a011-eca3	STALE	eth-0-1

12.3 DHCPv6 Relay Configuration

12.3.1 Introduction

If the DHCPv6 server and clients are in a same subnet, DHCPv6 protocol interaction can be directly realized between the clients and server, without enabling DHCPv6 relay. If the DHCPv6 server and clients are not in a same subnet, it is needed to enable DHCPv6 relay to forward DHCPv6 messages to the external DHCPv6 server.

DHCP relay forwarding differs from normal IPv6 routing transfer. The IPv6 data packets forwarded via IPv6 routing transfer are exchanged between networks transparently, while DHCPv6 relay will generate a new DHCPv6 message and send it to another interface while receiving a DHCPv6 message. DHCPv6 relay sets relay address and adds relay (remote-id) information in messages, and sends it to the DHCPv6 server end.

12.3.2 Topological Graph

The figure below shows the network topology of testing DHCPv6 relay agent, for which two PCs and one switch are needed to construct the testing environment.

- Computer A acts as DHCPv6 server
- Computer B acts as DHCPv6 client
- Switch acts as DHCPv6 relay

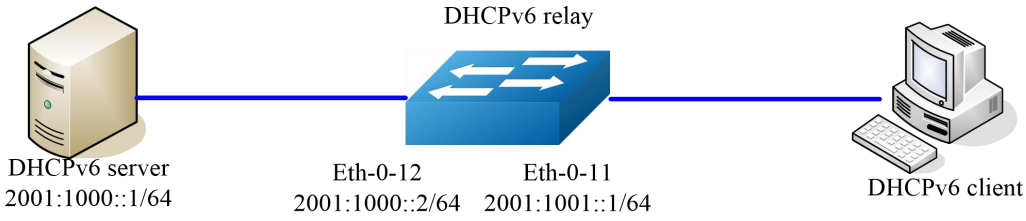


Figure 12-9: DHCPv6 Relay Topological Graph

12.3.3 Configuration

Enable DHCPv6 Relay Global Service

Switch(config)# service dhcpv6 enable	Enable DHCPv6 server
Switch(config)# dhcpv6 relay	Enable DHCPv6 Relay feature
Switch(config)# dhcpv6 relay remote-id option	Enable DHCPv6 Remote-id option
Switch(config)# dhcpv6 relay pd route	Enable DHCPv6 prefix-delegation route learning

Configure DHCPv6 server group

Switch(config)# dhcpv6-server 1 2001:1000::1	Create DHCPv6 server group

Configure interface eth-0-12

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-12	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# ipv6 address 2001:1000::2/64	Set IPv6 address
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# exit	Exit interface configuration mode

Configure interface eth-0-11

Switch(config)# interface eth-0-11	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface.
Switch(config-if)# ipv6 address 2001:1001::1/64	Set IPv6 address
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# dhcpv6-server 1	Configure DHCPv6 server group
Switch(config-if)# exit	Exit interface configuration mode

12.3.4 Command Validation

Step 1 Check interface configuration.

```
Switch# show running-config interface eth-0-12
!
interface eth-0-12
 no switchport
 ipv6 address 2001:1000::1/64

!

Switch # show running-config interface eth-0-11
!
interface eth-0-11
 no switchport
 ipv6 address 2001:1001::1/64
 dhcpv6-server 1
!
```

Step 2 Check DHCPv6 server status.

```
Switch# show services
Networking services configuration:
Service Name        Status
============================================================
dhcp                disable
dhcpv6               enable
```

Step 3 Check DHCPv6 server group configuration.

```
Switch# show dhcpv6-server
DHCPv6 server group information:
============================================================
group 1 ipv6 address list:
[1] 2001:1000::1
```

Step 4 Show DHCPv6 relay statistics.

```
Switch# show dhcpv6 relay statistics
```

```
DHCPv6 relay packet statistics:
============================================================
Client relayed packets  :  8
Server relayed packets :  8
Client error packets      :  0
Server error packets     :  0
```

Step 5 Show prefix-delegation client information as recorded.

```
Switch# show dhcpv6 relay pd client
DHCPv6 prefix-delegation client information:
============================================================
Interface  : eth-0-11
Client DUID  : 000100011804ff38c2428f04970
Client IPv6 address  : fe80::beac:d8ff:fedf:c600
   IA ID  : d8dfc60
      IA Prefix :  2002:2:9:eebe::/64
         prefered/max lifetime : 280/300
         expired time :  2001-1-1 09:10:58
============================================================
```

13 IPv6 Multicast Configuration Guide

13.1 IPv6 Multicast-Routing Configuration

13.1.1 Introduction

With the continuous development of the Internet, many interactive services such as network data, voice and video information are steadily on the increase. Besides, services requiring high bandwidth and real-time data interaction performance such as emerging e-business, online meeting, online auction, video on demand and distance teaching rise gradually, which demand more in respect of information security, accountability and network bandwith.

The situation where the efficiency of unicast and broadcast will be low if the number of users needing certain information in the network is uncertain has been changed by the emergence of the IPv6 multicast technology. Where some users in the network need specific information, multicast information sender (namely multicast source) will send information once only and establish a tree based routing with multicast routing protocol for multicast data packets, and the transmitted information will not be copied and distributed until reaching the node as close as possible to the user side.

With a multicast routing protocol, multiple receivers can receive multicast data across various networks.

- MLD (multicast listener discovery) is a protocol belonging to IPv6 protocol family for IPv6 multicast member management. It is used to establish and maintain multicast member relationships between IPv6 host and its direct adjacent multicast router.
- PIMv6 (Protocol Independence Multicast) is applied between multicast routers or between multilayer switches. The unicast routing protocol routing IPv6 multicast can be static routing, RIPng or OSPFv3, multicast routing and unicast routing are protocol independent as long as unicast routing protocol can generate routing table entries. By virtue of the RPF (Reverse Path Forwarding) mechanism, PIMv6 has realized multicast information transfer in the network. To facilitate describing, the network composed with multicast routers supporting PIMv6 protocol is called PIMv6 multicast domain. PIMv6 is classified into dense mode and sparse mode, and we support sparse mode only for the moment.

13.1.2 Configuration

We can support multicast routing table with a limit of 2048 entries by default.

Switch# configure terminal	Enter configuration mode

Switch(config)# ipv6 multicast route-limit 1000	Configure maximum multicast entry limit

13.1.3 Check Configuration

```
Switch# show ipv6 mroute 2001:1::1234

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
2001:1::1234, ff0e::1234:5678
uptime 00:00:31, stat expires 00:03:08
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
    eth-0-2
2001:1::1234, ff0e::6666:6666
uptime 12:00:00 AM, stat expires 12:03:30 AM
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
```

13.2 MLD Configuration

13.2.1 Introduction

The host, router and multilayer switch participating in IPv6 multicast must have the MLD feature. This protocol defines querier and host role:

- The querier of network devices sends query messages to a specific group in the network to discover multicast members.
- The host sends MLD report message (to respond to the query messages) to notify the querier that the host will join in corresponding multicast group list.
- The members of a multicast group are dynamic, and the host can join and exit at any time. No limitation is set on the position or count of multicast members.

A host can act as a member of multiple multicast groups. At the same time, members are active in the multicast groups, which can change with group and with the time. A multicast group can last a long time or briefly.

MLD messages use the following multicast addresses:

- ff02::1 as destination address (all systems in a subnet) for query by general MLD group.
- Group-specific MLD address as destination address for an IPv6 group-specific query.
- MLD group members send Report messages to specific multicast IPv6 addresses.
- MLDv1 sends an exit message to ff02::2 at the time of exiting the multicast group.

13.2.2 References

MLD module is based on the following RFCs

- RFC 2710
- RFC 3810

13.2.3 Configuration

Enabling MLD is dependent on enabling multicast routing protocol. MLD will be automatically enabled once PIMv6 or other multicast routing protocols are enabled on the interface, and vice versa. Please note that IPv6 multicast routing must be enabled in global mode before MLD runs. The system supports dynamic learning MLD group records, and configuring static MLD group records.

Enable MLD

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 multicast-routing	Enable multicast routing in global mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Set IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface

Configure MLD Interface Parameters

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Access interface mode
Switch(config-if)# ipv6 mld version 2	Set MLD version
Switch(config-if)# ipv6 mld query-interval 120	Set MLD query interval
Switch(config-if)# ipv6 mld query-max-response-time 12	Set maximum MLD query response time
Switch(config-if)# ipv6 mld robustness-variable 3	Set MLD robustness
Switch(config-if)# ipv6 mld last-member-query-count 3	Set MLD last member query count
Switch(config-if)# ipv6 mld last-member-query-interval 2000	Set MLD last member query interval

Configure Maximum MLD Group Limit

You can globally configure the maximum MLD group limit or configure the maximum MLD group limit in interface mode.

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 mld limit 2000	Configure global maximum MLD group limit
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ipv6 mld limit 1000	Set maximum MLD group limit in interface mode

Configure Static MLD Group

You can configure a static MLD group in interface mode.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ipv6 mld static-group ff0e::1234	Configure static MLD group

Configure MLD Proxy

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface
Switch(config-if)# ipv6 mld proxy-service	Set the interface as upstream port of MLD proxy
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1	Set eth-0-2 as downstream port of MLD proxy, and eth-0-1 as upstream port of MLD proxy

13.2.4 Check Configuration

Show MLD Interface Information

```
Switch# show ipv6 mld interface
Interface eth-0-1 (Index 1)
 MLD Active, Querier, Version 1 (default)
 Internet address is fe80::8c8e:dbff:feef:1900
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
Interface eth-0-9 (Index 9)
 MLD Active, Querier, Version 1 (default)
 Internet address is fe80::8c8e:dbff:feef:1900
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
```

Show MLD Group Information

```
Switch# show ipv6 mld groups
MLD Connected Group Membership
Group Address                Interface        Expires
ff0e::1234:5678              eth-0-2          00:03:01
```

13.3 PIMv6-SM Configuration

13.3.1 Introduction

Protocol independent multicast sparse mode (PIMv6-SM) is a multicast routing protocol for connecting sparsely distributed multicast devices for collaboration.' It helps sparse network nodes save bandwidth and reduce bandwidth usage by transmitting a single flow to multiple receivers.

PIMv6-SM uses receivers to initiate members' IPv6 multicast mode, which supports the shared and shortest path tree and uses the soft-state mechanism to adapt to the constantly changing network condition. It relies on unicast routing protocol for establishing and maintaining multicast routing between routers.

13.3.2 References

PIMv6-SM module is based on the following IETF standard:

RFC 4601

13.3.3 Terms

The concepts related to in PIMv6-SM protocol are briefed below:

Rendezvous Point

Rendezvous point (RP) acts as the rendezvous point of multicast in SM mode, and senders and recipients rendzvous at the RP. Every multicast router must know the RP specific to each multicast group.

All multicast data must be registered with RP, and all receivers who need multicast data can request data by sending a JOIN message to the RP. The source registration mechanism is to inform the RP of the sources of data in the network.

Multicast Routing Information Base (MRIB)

Multicast routing list is obtained based on unicast routing table. In PIMv6-SM, MRIB is used to determine the target of sending join/prune messages. It also provides routing metrics of destination work. These metrics will be used when sending and processing Assert messages.

Reverse Path Forwarding

RPF means a router for receiving data packet from Source A passing through interface IF1 will receive the data packet only if interface IF1 is the egress interface for reaching Source A. RPF uses unicast routing table to determine whether the ingress port is correct. The data packet is forwarded because the unicast routing table indicates that interface IF1 is the shortest path to Source A. Unicast routing table selects the shortest path for multicast data.

Multicast Tree Information Base (TIB)

TIB is an information base on multicast router for storing all multicast forwarding tree information, which is built by receiving PIMv6 join/prune messages, Assert messages and MLD messages.

Upstream

It is near the tree root, and the tree root may be a source or RP.

Downstream

It is away from the tree root, and the tree root may be a source or RP.

Source-based Tree

The forwarding path of source-based tree is the shortest forwarding path to the source. If the unicast routing metrics is a hop, the forwarding path of source-based tree is the minimum hop; if the unicast routing metrics is delay, the forwarding path of source-based tree is the minimum delay.

For each multicast source, a corresponding multicast forwarding tree is provided to directly connect the source with receivers. All flows transmitted to the designated group are forwarded along the corresponding forwarding tree.

Shared Tree

Shared tree depends on RP. All flows are transmitted from a source to an RP, and the RP transmits the flows to receivers. For each multicast group, only one forwarding tree is established, regardless of the count of sources. Shared tree is unidirectional, so that traffic flows from the RP to receivers only. If multicast data from a source is to be transmitted, the multicast data will be transmitted to an RP, and then to receivers from the RP.

BootStrap Router

When a multicast source starts sending multicast data or a receiver starts sending a join message to an RP, the multicast router must know the RP information. BSR is responsible for gathering RP information in the network upon PIMv6-SM network startup, electing an RP for each group, and distributing RP set (namely group-RP mapping database) across the entire PIMv6-SM network.

Data Flow from Source to Receiver

Sending Hello message

PIMv6 router regularly sends a Hello message to discover PIMv6 router neighbors. Hello message is a multicast message using an address offf02::d. PIMv6 router responds to Hello messages, and the hold time of Hello messages determines the active time of the messages.

Electing Designated Router

If there are multiple multicast routers in a multi-access network, only one multicast router will be elected as the designated router to send join/prune messages to an RP for multicast receivers in local network.

RP Discovery

PIMv6-SM generates bootstrap message via bootstrap router and distributes RP message to all multicast routers. Multicast routers receive and store bootstrap messages. When DR receives an MLD message or multicast data from a direct-connected host, DR will calculate out the RP of the multicast group, and send a join/prune message to RP or encapsulate register message to the RP. Static assigning RP is supported for small network environment.

Joining Shared Tree

To join a multicast group, the host will send an MLD message to the upstream router, and the multicast router will send a join message to the upstream PIMv6 neighbor in the RP direction. Multicast router will check whether there is a local multicast group upon receiving the join request from the downstream devices. If there is a local multicast group, it means that the join message has been transmitted to the shared tree, and the interface receiving the message becomes an outgoing interface. If there is no local multicast group, entries will be created, the interface receiving the message is added into the outgoing, and the join message will be sent to the upstream PIMv6 neighbor in the RP direction.

Multicast Source Registration

The router directly connected to multicast source S, upon receiving a message from the multicast, will encapsulate the message into a register message and send it to the corresponding RP in unicast mode. When the RP receives the register message from multicast source S, it will de-encapsulate the register message and forward multicast information along RPT tree to receivers, and also send a join message to multicast source hop-by-hop (S, G) so as to enable all routers between the RP and multicast source to generate table entries (S, G). The routers passed through form branches of SPT tree. SPT source tree takes multicast source S as the root, and the

RP as destination. The multicast information from multicast source S reaches the RP along the established SPT tree, and the RP forwards the information along RPT shared tree.

Sending Register-Stop Message

If an RP receives a register message from the multicast source and an unencapsulated multicast message thereafter, the RP will send a register-stop message to DR near the multicast source, and DR will stop sending register message to the RP upon receiving the register-stop message.

Prune Port

The multicast router on the receiver side sends a prune message to the upstream PIMv6 neighbor in the RP direction. The uplink multicast router, upon receiving the prune message, will delete the interface receiving the prune message as forwarding port. If no other receivers exist on the router, sending prune message to the upstream PIMv6 neighbor in the RP direction will continue.

Forwarding Multicast Data

PIMv6-SM router sends multicast data to those explicitly intending to join the multicast group.

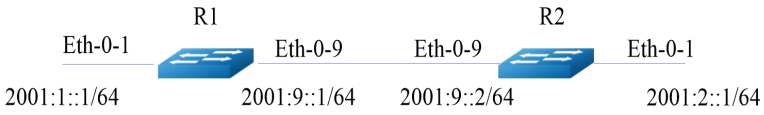
Multicast router will conduct RPF check, and only the qualified multicast data packets can be sent out via the outgoing port.

13.3.4 Configure General PIMv6 Sparse-mode

I. Configuration

PIMv6-SM is a soft-state protocol. The essential requirement is to enable PIMv6-SM protocol on the needed interfaces and correctly configure RP information in static or dynamic manner. The MLD report/exit and PIMv6 join/prune messages of all multicast groups remain dynamic. We only support all multicast groups of one RP at the moment (224.0.0.0 / 4).

This section provides two related scenes of PIMv6-SM configuration. The network topology used for the example is as follows:



Configure Static RP

In the example above, R1 is an RP, and all routers are configured with a static RP;

- Every router is configured with a static RP address 2001:1::1.
- PIMv6-SM feature must be enabled on all interfaces.

R1

Switch# configure terminal	Enter configuration mode

Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:9::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# ipv6 route 2001:2::/64 2001:9::2	Configure static unicast route
Switch(config)# ipv6 pim rp-address 2001:1::1	Configure static RP address

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:2::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:9::2/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface

Switch(config-if)# exit	Exit interface mode
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	Configure static unicast route
Switch(config)# ipv6 pim rp-address 2001:1::1	Configure static RP address

II. Check configuration

All routers are configured with the same RP address 2001:1::1, and the following commands are used to validate the RP configuration, interface details and multicast routing table.

Detailed RP Description

The result of running command “show PIMv6-SM RP mapping” on R1 indicates that 11.1.1.1 is the RP configured to all multicast groups 224.0.0.0/4 in static manner. All other routers have a similar output:

R1# show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
Group(s): ff00::/8, Static
  RP: 2001:1::1
    Uptime: 12:00:04 AM
Embedded RP Groups:
```

Interface Details

Show multicast information of R1 interface.

R1# show ipv6 pim sparse-mode interface

```
Interface   VIFindex Ver/   Nbr   DR
                     Mode   Count  Prior
eth-0-1     2        v2/S   0      1
  Address       : fe80::fc94:efff:fe96:2600
  Global Address: 2001:1::1
  DR            : this system
eth-0-9     0        v2/S   0      1
  Address       : fe80::fc94:efff:fe96:2600
  Global Address: 2001:9::1
  DR            : this system
```

IPv6 Multicast Routing Table

Show PIMv6-SM multicast routing table.

R1# show ipv6 pim sparse-mode mroute detail

```
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
```

```
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:01:37
  RP: 2001:1::1, RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT: off
   Macro state: Join Desired,
  Downstream:
   eth-0-1:
    State: NO INFO, ET: off, PPT: off
    Assert State: NO INFO, AT: off
     Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
    Macro state: Could Assert, Assert Track
  Local Olist:
   eth-0-1
```

R2# show ipv6 pim sparse-mode mroute detail

```
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 12:00:06 AM
  RP: 2001:1::1, RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT: off
   Macro state: Join Desired,
  Downstream:
   eth-0-1:
    State: NO INFO, ET: off, PPT: off
    Assert State: NO INFO, AT: off
     Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
    Macro state: Could Assert, Assert Track
  Local Olist:
   eth-0-1
```

13.3.5 Configure Dynamic RP

In small and simple network, the amount of information is small, and only one RP is needed in the whole network for forwarding information, where the RP position can be specified on routers in SM domain in static manner. In many conditions, however, PIMv6-SM network is of a large size, and a huge amount of information will be forwarded via RP. To relieve the RP load and optimize the topological structure of the shared tree, different multicast groups should have separate RPs. In this case, the bootstrap mechanism is needed for electing an RP in dynamic manner.

I. Configuration

The below shows detailed configuration of a dynamic RP:

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:9::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enter configuration mode
Switch(config-if)# exit	Enter interface mode
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	Configure static unicast route
Switch(config)# ipv6 pim rp-candidate eth-0-1	Configure candidate RP interface

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:2::1/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode

Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:9::2/64	Configure IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM on interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	Configure static unicast route
Switch(config)# ipv6 pim rp-candidate eth-0-9	Configure candidate RP interface
Switch(config)# ipv6 pim bsr-candidate eth-0-9	Configure candidate BSR interface

Select the router of top priority as RP. If two or more routers share the same priority, the Hash Function in BSR mechanism can be used to select RP to ensure that all routers in PIMv6 domain match the same RPs of a group. Use the "**ipv6 pim rp-candidate IFNAME PRIORITY**" command to change the default priority of candidate RP.

II. Check configuration

PIMv6-SM's Group-RP Mapping Relation

Use command "**show ipv6 pim sparse-mode rp mapping**" to show details of Group-RP mapping, and the output is candidate RP information. The group of ff00::/8 is provided with two candidate RPs. The default priority of candidate RP 2001:1::1 is 192, and the priority of candidate RP 2001:9::2 is configured as 2. Being of a higher priority, candidate RP 2001:1::1 is selected as the RP of multicast group ff00::/8.

R2# show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::2, via bootstrap, priority 2
        Uptime: 12:00:32 AM, expires: 12:02:02 AM
  RP: 2001:1::1
    Info source: 2001:1::1, via bootstrap, priority 192
        Uptime: 12:00:31 AM, expires: 12:02:03 AM
Embedded RP Groups:
```

Detailed RP Display

To display the information of group-specific RP routers, please use the following command. The output indicates that 2001:9::2 has selected the RP for ff02::1234 multicast group.

R2# show ipv6 pim sparse-mode rp-hash ff02::1234

RP: 2001:9::2
Info source: 2001:9::2, via bootstrap

RP information will reach all PIMv6 routers in the domain, and the state machines will keep all results of routing join/prune from group members. For displaying detailed interface information and multicast routing table information, please refer to the part of Static RP Configuration above.

13.3.6 Configure Bootstrap Router

Each multicast group needs an RP to serve it, and the RP is taken as the root of the distribution tree based on multicast group. To ensure multicast data from the sender can reach receivers, the multicast routers in one multicast domain need to use the same multicast group-RP mapping. To select an RP for a specific multicast group, multicast routers need to maintain a series of multicast-RP mapping relations, which is called RP set. The mechanism of bootstrap router is to enable multicast routers in the same multicast domain to learn the RP set.

BSR is the core of management in PIMv6-SM network, mainly responsible for:

- Gathering advertisement messages from Candidate-RP (C-RP) in the network.
- Selecting partial C-RP information for each multicast group and forming an RP-Set (namely multicast group-RP mapping database).
- Notifying all routers (including DR) across the whole PIMv6-SM network of the RP position.

One PIMv6 domai n needs one or more candidate BSRs, and a bootstrap router BSR will be automaticall elected from the candidate BSRs to be responsible for gathering and distributing RP information. The below briefs automatic election from candidate BSRs:

- An interface with PIMv6-SM enabled must be assigned while configuring a router as candidate BSR.
- All candidate BSRs initially regard themselves as a BSR of the IPv6-SM and sends bootstrap messages with IPv6 address of the interface as BSR address.
- Candidate BSRs will compare the BSR address of the newly received bootstrap message with their own BSR address when receiving a bootstrap message from other routers for priority and IPv6 address. With the same priority, the larger IPv6 address is regarded better. If the former is better, Candidate BSRs will replace its own BSR address with the new BSR address, and stop regarding themselves as a BSR. Otherwise, they will retain their own BSR address, and continue to regard themselves as a BSR.
- The alternative RP reports its own RP information to the bootstrap router, and the bootstrap router distributes the aggregated RP set to all routers across the multicast domain via bootstrap message.

I. Topology

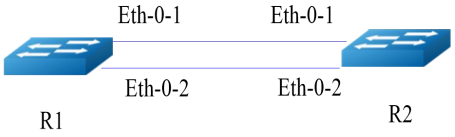


Figure 13-1 BSR Topology

II. Configuration

Router 1

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 pim bsr-candidate eth-0-1	Assign candidate BSR interface, with a priority of 64 by default

Router 2

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 pim bsr-candidate eth-0-1 10 25	Configure BSR candidate interface with HASH mask length of 10 and priority of 25
Switch(config)# ipv6 pim rp-candidate eth-0-1 priority 0	Configure RP candidate interface with priority of 0

Use command "**ipv6 pim unicast-bsm**" to configure the interface to send and receive BSM messages in unicast manner.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ipv6 pim dr-priority 10	Configure the priority of interface DR
Switch(config-if)# ipv6 pim unicast-bsm	Configure the interface to send and receive BSM messages in unicast manner

III. Check configuration

Check Candidate BSR Router

Switch# show ipv6 pim sparse-mode bsr-router

```
PIM6v2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2001:9::1 (?)
  Uptime:      12:01:27 AM, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 12:00:16 AM
  Role: Candidate BSR
  State: Elected BSR
```

Check Candidate BSR Router

```
Switch# show ipv6 pim sparse-mode bsr-router
PIM6v2 Bootstrap information
  BSR address: 2001:9::1 (?)
  Uptime:      12:01:34 AM, BSR Priority: 64, Hash mask length: 126
  Expires:     12:01:51 AM
  Role: Candidate BSR
  State: Candidate BSR
  Candidate RP: 2001:9::2(eth-0-9)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:35
```

Check RP on E-BSR

```
Switch# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::2, via bootstrap, priority 0
        Uptime: 12:45:37 AM, expires: 12:02:29 AM
Embedded RP Groups:
```

Check RP on C-BSR

```
Switch# show ipv6 pim sparse-mode rp mapping

PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::1, via bootstrap, priority 0
        Uptime: 12:03:14 AM, expires: 12:01:51 AM
Embedded RP Groups:
```

13.3.7 Configure PIMv6-SSM

PIMv6-SSM and PIMv6-SM can work together on multicast routers. PIMv6-SSM is disabled by default.

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 pim ssm default	Enable PIMv6-SSM
Switch(config)# ipv6 pim ssm range ipv6acl	Set PIMv6-SSM group range according to

	the assigned ipv6acl

13.4 PIMv6-DM Configuration

13.4.1 Introduction

Protocol independent multicast dense mode (PIMv6-DM) is a multicast routing protocol for connecting densely distributed multicast devices for collaboration.' It helps sparse network nodes save bandwidth and reduce bandwidth usage by transmitting a single flow to multiple receivers.

PIMv6-DM assumes that when a multicast source starts sending multicast stream, all downstream systems expect to receive the multicast stream. In the beginning, the multicast stream floods across the entire network. In the case of flooding, PIMv6-DM uses RPF to prevent loops of multicast stream. If there is no receiving member of the multicast group in some network zones, PIMv6-DM will delete the forwarding branch by means of pruning.

Pruning state is subjec to a life cycle. Upon the life cycle ending, multicast data will start forwarding again. The multicast group corresponding to each (S,G) has its own pruning state. If a new recipient appears in a pruned zone of a multicast group, the router will change the pruning state to forwarding path by sending a "graft" message to the multicast source.

13.4.2 References

PIMv6-DM module is based on the following IETF standard:

RFC 3973

13.4.3 Configure General PIMv6 Dense-mode

I. Topology

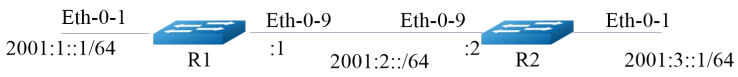


Figure 13-2 Configure PIMv6 dense-mode

II. Configuration

PIMv6-DM is a soft-state protocol. The essential requirement is to enable PIMv6-DM protocol on the needed interfaces. The state of all multicast groups is maintained in dynamic manner via MLD report/exit and PIMv6 messages.

This section provides one related scene of PIM-DM configuration. The network topology used for the example is as above:

Multicast stream enters via R1 eth-0-1, and receivers connect to R2 eth-0-2.

The configuration examples are as below:

Configuring R1

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# interface eth-0-1	Enter interface mode of eth-0-1
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Configure interface IPv6 address
Switch(config-if)# ipv6 pim dense-mode	Enable interface pimv6 dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode of eth-0-9
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:2::1/64	Configure interface IPv6 address
Switch(config-if)# ipv6 pim dense-mode	Enable interface pimv6 dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# ipv6 route 2001:3::/64 2001:2::2	Configure a static routing

Configuring R2

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 enable	Enable IPv6
Switch(config)# interface eth-0-1	Enter interface mode of eth-0-1
Switch(config-if)# no shutdown	Enable the interface
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:3::1/64	Configure interface IPv6 address
Switch(config-if)# ipv6 pim dense-mode	Enable interface pimv6 dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# interface eth-0-9	Enter interface mode of eth-0-9
Switch(config-if)# no shutdown	Enable the interface

Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ipv6 address 2001:2::2/64	Configure interface IPv6 address
Switch(config-if)# ipv6 pim dense-mode	Enable interface pimv6 dm feature
Switch(config-if)# exit	Exit interface mode
Switch(config)# ipv6 route 2001:1::/64 2001:2::1	Configure a static routing

III. Check configuration

Use the following commands to check interface configuration and routing table information.

Interface Details

Use command “show ipv6 pim dense-mode interface” to display interface details on R1.

```
R1# show ipv6 pim dense-mode interface
Neighbor Address                Interface   VIFIndex Ver/   Nbr
                                                     Mode   Count
fe80::326f:c9ff:fef2:8200       eth-0-1     0        v2/D   0
fe80::326f:c9ff:fef2:8200       eth-0-9     2        v2/D   1
```

Neighbor Details

Use command “show ipv6 pim dense-mode neighbor” to display neighbor details on R1

```
R1# show ipv6 pim sparse-mode neighbor
Neighbor Address                Interface   Uptime/Expires    Ver
fe80::ce47:6eff:feb7:1400       eth-0-9     00:51:51/00:01:24 v2
```

Multicast Routing Table Information

Use command “show ipv6 pim dense-mode mroute” to display the details of PIM-DM multicast routing table

R1# show ipv6 pim dense-mode mroute

```
PIM-DM Multicast Routing Table
(2001:1::2, ff0e::1)
  Source directly connected on eth-0-1
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-1
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-9, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

R2# show ipv6 pim dense-mode mroute

```
PIM-DM Multicast Routing Table
(2001:1::2, ff0e::1)
  RPF Neighbor: none
  Upstream IF: eth-0-9
    Upstream State: AckPending
    Assert State: Loser
  Downstream IF List:
    eth-0-1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

13.5 Configure MLD Snooping

13.5.1 Introduction

MLD Snooping (mlticast listener discovery snooping) is an IPv6 multicast constraint mechanism running on layer 2 Ethernet switches for managing and controlling IPv6 multicast groups.

Layer 2 switches control flooding of IPv6 multicast stream via MLD Snooping. If a layer 2 Ethernet switch receives an MLD message transmitted between a host and routers, MLD Snooping will analyze the information in the MLD message, establishing a mapping relationship between the interface and IPv6 multicast address, and forward IPv6 multicast data according to this mapping relationship. IPv6 Multicast routers regularly send general group query to maintain IPv6 multicast group member relationship. All receivers will respond to the query by sending an MLD report message, and switches establish forwarding table entries by snooping the MLD report message.

Layer 2 multicast group can be established in dynamic manner via MLD message or configured in static manner. Statically configured multicast groups will override dynamic multicast groups.

13.5.2 Configure Enabling MLD Snooping

MLD Snooping can be enabled globally or individually in each VLAN. If MLD Snooping is disabled in global mode, MLD Snooping will be inactive even if you enable IGMP Snooping individually in all VLANs. Suppose MLD Snooping is enabled in global mode. You can disable MLD Snooping in one VLAN. Besides, global configuration can override configurations of all VLANs. By default, MLD Snooping is disabled in global mode and individually in each VLAN.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping	Enable MLD Snooping in global mode
Switch(config)#ipv6 mld snooping vlan 1	Enable MLD Snooping in individual VLAN
Switch # show ipv6 mld snooping vlan 1	Check configuration

II. Command validation

Switch # show ipv6 mld snooping vlan 1

```
Global Mld Snooping Configuration
----------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Report-Suppression             :Enabled
Vlan 1
----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

13.5.3 Configure MLD Snooping Quick Leave

Under normal circumstances, MLD Snooping will not directly delete an interface from a multicast group after receiving an MLD exit message, but send an MLD group-specific query message and delete the interface from the multicast group if no response is received after a period of time. If the quick delete function is enabled, MLD Snooping will directly delete an interface from a multicast group upon receiving an MLD message. If there is only one user under the interface, quick delete helps saving bandwidth.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)#ipv6 mld snooping fast-leave	Enable fast leave in global mode
Switch(config)#ipv6 mld snooping vlan 1 fast-leave	Enable fast leave in VLAN mode
Switch # show ipv6 mld snooping vlan 1	Check configuration

II. Command validation

```
Switch # show ipv6 mld snooping vlan 1
Global Mld Snooping Configuration
----------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
```

```
Mld Snooping Report-Suppression        :Enabled
Vlan 1
----------
Mld Snooping                           :Enabled
Mld Snooping Fast-Leave                :Enabled
Mld Snooping Report-Suppression        :Enabled
Mld Snooping Version                   :1
Mld Snooping Max-Member-Number         :4096
Mld Snooping Unknown Multicast Behavior :Flood
Mld Snooping Group Access-list         :N/A
Mld Snooping Mrouter Port              :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

13.5.4 Configure MLD Snooping Query Parameters

Layer 3 switches periodically send general MLD query messages in the connected network segment, and learn about which multicast groups have members in the segment by resolving the returned MLD host report messages. Multicast routers periodically send query messages and refresh the corresponding group member relationship information in the network segment when receiving an MLD host report message from a group member.

I. Configuration

Switch #configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping query-interval 100	Set query interval as 100 seconds
Switch(config)# ipv6 mld snooping query-max-response-time 5	Set maximum response time as 5 seconds
Switch(config)#ipv6 mld snooping last-member-query-interval 2000	Set last member query interval
Switch(config)#ipv6 mld snooping vlan 1 querier address fe80::1	Configure MLD Snooping querier address on VLAN1
Switch(config)#ipv6 mld snooping vlan 1 querier	Enable MLD Snooping querier on VLAN1
Switch(config)#ipv6 mld snooping vlan 1 query-interval 200	Set query interval of VLAN1 as 200 seconds
Switch(config)#ipv6 mld snooping vlan 1 query-max-response-time 5	Set maximum response time of VLAN1 as 5 seconds
Switch(config)#ipv6 mld snooping vlan 1 querier-timeout 100	Set queirer timeout of VLAN1 as 100 seconds
Switch(config)#ipv6 mld snooping 1 last-member-query-interval 2000	Set group-specific query interval of VLAN1 as 2000 seconds
Switch(config)# ipv6 mld snooping vlan 1 discard-unknown	Discard unknown multicast messages on VLAN1

Switch(config)# ipv6 mld snooping discard-unknown	Discard unknown multicast messages in global mode

II. Command validation

```
Switch # show ipv6 mld snooping querier
Global Mld Snooping Querier Configuration
-------------------------------------------------
Version                                 :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)                    :100
Global Source-Address                   :::
TCN Query Count                         :2
TCN Query Interval (sec)                :10
Vlan 1:   MLD snooping querier status
-----------------------------------------------
Elected querier is : fe80::1
-----------------------------------------------
Admin state                             :Enabled
Admin version                           :1
Operational state               :Querier
Querier operational address     :fe80::1
Querier configure address       :fe80::1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)                    :200
Querier-Timeout (sec)                   :100
```

13.5.5 Configure MLD Snooping Multicast Routed Ports

Multicast routed ports refer to switch ports connecting to multicast routers, which can be dynamically learned or statically configured. If a port of a VLAN receives a general MLD query message or PIMv6 Hello message, the port becomes the multicast routed port of the VLAN. All MLD query messages received via multicast routed port will be broadcast in the VLAN. All MLD report/exit messages received on the VLANs also will be forwarded from the multicast routed port (with message suppression disabled), and all multicast flows received from the VLAN will be forwarded from the multicast routed port.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping report-suppression	Enable MLD Snooping report suppression
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface eth-0-1	Configure static multicast router interface
Switch(config)# ipv6 mld snooping vlan 1 report-suppression	Enable report suppression on VLAN1

Switch(config)# ipv6 mld snooping vlan 1 mrouter-aging-interval 200	Configure dynamic multicast router aging interval

II. Command validation

```
Switch# show ipv6 mld snooping vlan 1
Global Mld Snooping Configuration
---------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Discard
Mld Snooping Report-Suppression             :Enabled
Vlan 1
-----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Discard
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :200
```

13.5.6 Configure MLD Snooping Query TCN

Multicast group learning and updating after STP convergence topology can be adapted to by configuring TCN interval and query count.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping querier tcn query-count 5	Set TCN query count
Switch(config)# ipv6 mld snooping querier tcn query-interval 20	Set TCN query interval as 20 seconds

II. Command validation

```
Switch # show ipv6 mld snooping querier
Global Mld Snooping Querier Configuration
---------------------------------------------------
Version                     :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :100
```

```
Global Source-Address              :::
TCN Query Count                    :5
TCN Query Interval (sec)           :20
Vlan 1:   MLD snooping querier status
-----------------------------------------------
Elected querier is : fe80::1
-----------------------------------------------
Admin state                        :Enabled
Admin version                      :1
Operational state                  :Querier
Querier operational address        :fe80::1
Querier configure address          :fe80::1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)      :5
Query-Interval (sec)               :200
Querier-Timeout (sec)              :100
```

13.5.7 Configure MLD Snooping Report Suppression

Switches use MLD report suppression to prevent repeatedly sending same MLD messages to multicast routers. If MLD router suppression is enabled (by default), a switch sends the first MLD report message to a multicast router, and other same MLD report messages will not be sent to the multicast router. In this way, duplicate MLD report messages will not be sent to the multicast router.

I. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping report-suppression	Enable report suppression in global mode
Switch(config)# ipv6 mld snooping vlan 1 report-suppression	Enable report suppression in VLAN1 mode

II. Command validation

Switch # show ipv6 mld snooping

```
Global Mld Snooping Configuration
---------------------------------------------------
Mld Snooping                              :Enabled
Mld Snooping Fast-Leave                   :Disabled
Mld Snooping Version                      :2
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Flood
Mld Snooping Report-Suppression           :Enabled
Vlan 1
----------
Mld Snooping                              :Enabled
Mld Snooping Fast-Leave                   :Disabled
Mld Snooping Report-Suppression           :Enabled
```

```
Mld Snooping Version                          :2
Mld Snooping Max-Member-Number                :4096
Mld Snooping Unknown Multicast Behavior       :Flood
Mld Snooping Group Access-list                :N/A
Mld Snooping Mrouter Port                     :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

13.5.8 Configure Static Multicast Group

Switches will establish MLD Snooping group records when receiving MLDmessages via layer 2 ports. The current system also supports statically configuring MLD Snooping group records, for which group address, layer 2 port and the VLAN of the layer 2 port must be assigned.

I. Configuration

Switch#configure terminal	Enter configuration mode
Switch(config)# ipv6 mld snooping vlan 1 static-group ff0e::1234 interface eth-0-2	Configure static multicast group ff0e::1234, and vlan1 eth-0-2 as member interface

II. Command validation

Switch# show ipv6 mld snooping groups

VLAN	Interface	Group Address	Uptime	Expire-time
1	eth-0-2	ff0e::1234	00:00:02	stopped

13.5.9 Restriction and Configuration Guide

Multicast IPv6 is used in VRRP, RIPng and OSPFv3 protocols. Be sure not to use such multicast IPv6 in networks with MLD Snooping enabled, because the mapped MAC of such multicast IPv6 is consistent with that of the multicast IPv6 used by protocol module.

VRRP uses ff02::12, so the mapped multicast IPv6 of multicast MAC 3333.0000.0012 should be avoided in MLD Snooping and VRRP networks.

RIPv6 uses ff02::9, so the mapped multicast IPv6 of multicast MAC 3333.0000.0009 should be avoided in MLD Snooping and RIPng networks.

OSPF uses ff02::5, so the mapped multicast IPv6 of multicast MAC 3333.0000.0005 should be avoided in MLD Snooping and OSPFv3 networks.

13.6 Configure MVR6

13.6.1 Introduction

In conventional IPv6 multicast-on-demand mode, some access switches are linked under an aggregation multicast router, and the access switches are connected with users distributed in different VLANs. When users from those VLANs request a program of a same group, the aggregation multicast router needs to make a copy of data for users in each VLAN, and the

multicast traffic from each VLAN will occupy the bandwidth of the access switches. This increases the load of the aggregation router and wastes the bandwidth of the access devices.

IPV6 Multicast VLAN registration (MVR6) feature can solve this problem well. Enable multicast VLAN on the access switch near the user side. The aggregation router needs to send multicast data in source VLAN to the access switch rather than make a copy in every user VLAN, and the access switch will make copies upon user request after receiving the multicast data and send a copy to users in every VLAN. This saves bandwidth usage and lowers the load of layer 3 devices.

MVR6's running relies on MLD Snooping, and will be valid in groups with MVR6 globally configured. If the multicast group in the MLD message received via the downstream port of MVR6 is not with MVR6 globally configured, the message will be ignored. Receiver information is maintained via MLD report/exit message received via the downstream port of MVR6. MVR6 upstream port will determine the VLANs for forwarding IPv6 multicast data based on the IPv6 multicast group information on the downstream port after receiving IPv6 multicast data.

13.6.2 Terms

MVR6: IPv6 Multicast VLAN registration

Source vlan: Source VLAN of multicast VLAN

Source port: Upstream port in MVR6 network for connecting with multicast router port

Receiver port: Downstream port in MVR6 network for connecting with receiver port

13.6.3 Topology

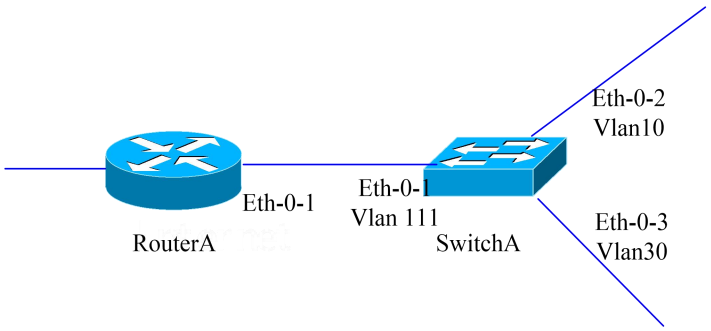


Figure 13-3 IPv6 Multicast VLAN Topology

13.6.4 Configuration

Destination

Enable MLD&PIMv6-SM on Router A eth-0-1.

Configure Switch A: eth-0-1 belongs to vlan111, eth-0-2 to vlan10 and eth-0-3 to vlan30.

Enable MVR6 on Switch A, make a copy of multicast stream from Router A to Switch A, and duplicate the multicast stream on Switch A and send it from eth-0-2 and eth-0-3.

Router A

Enable MLD&PIMv6-SM on configuration interface.

RouterA# configure terminal	Enter configuration mode
RouterA(config)# interface eth-0-1	Enter interface mode
RouterA(config-if)# no switchport	Set the interface as layer3 interface
RouterA(config-if)# no shutdown	Enable the interface
RouterA(config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address
RouterA(config-if)# ipv6 pim sparse-mode	Enable PIMv6-SM protocol
RouterA(config-if)# end	Go back to global mode

Switch A

Configure eth-0-1 to belong to vlan111, eth-0-2 to vlan10 and eth-0-3 to vlan30.

SwitchA# configure terminal	Enter configuration mode
SwitchA(config)# vlan database	Enter VLAN mode
SwitchA(config-vlan)# vlan 111,10,30	Create vlan 111, 10, 30
SwitchA(config-vlan)# quit	Exit VLAN mode
SwitchA(config)# interface vlan 111	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface vlan 10	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface vlan 30	Enter VLAN interface mode
SwitchA(config-if)# exit	Exit VLAN interface mode
SwitchA(config)# interface eth-0-1	Enter interface mode
SwitchA(config-if)# switchport access vlan111	Set the interface to belong to VLAN111
SwitchA(config)# interface eth-0-2	Enter interface mode
SwitchA(config-if)# switchport access vlan10	Set the interface to belong to VLAN10
SwitchA(config)# interface eth-0-3	Enter interface mode
SwitchA(config-if)# switchport access vlan30	Set the interface to belong to VLAN30
SwitchA(config-if)# end	Exit interface mode

Enable MVR6 on Switch A, so that only one copy of multicast stream will be made from Router A to Switch A, and the multicast stream will be sent from eth-0-2 and eth-0-3 on Switch A.

SwitchA# configure terminal	Enter configuration mode
SwitchA(config)# no ipv6 multicast-routing	Shut down IPv6 multicast routing
SwitchA(config)# mvr6	Enable MVR6
SwitchA(config)# mvr6 vlan 111	Create MVR6 VLAN
SwitchA(config)# mvr6 group ff0e::1234 64	Create IPv6 multicast group
SwitchA(config)# mvr6 source-address fe80::1111	Configure MVR6 source address
SwitchA(config)# interface eth-0-1	Enter interface mode
SwitchA(config-if)# mvr6 type source	Configure the interface as MVR6 source interface
SwitchA(config)# interface eth-0-2	Enter interface mode
SwitchA(config-if)# mvr6 type receiver vlan 10	Configure the interface as MVR6 receiver interface
SwitchA(config)# interface eth-0-3	Enter interface mode
SwitchA(config-if)# mvr6 type receiver vlan 30	Configure the interface as MVR6 receiver interface
SwitchA(config-if)# end	Exit interface mode

13.6.5 Command Validation

Router A

```
RouterA # show ipv6 mld groups
MLD Connected Group Membership
Group Address                Interface        Expires
ff0e::1234                   eth-0-2          00:03:01
ff0e::1235                   eth-0-2          00:03:01
ff0e::1236                   eth-0-2          00:03:01
ff0e::1237                   eth-0-2          00:03:01
ff0e::1238                   eth-0-2          00:03:01
……
ff0e::1273                   eth-0-2          00:03:01
```

Switch A

```
SwitchA# show mvr6
MVR6 Running: TRUE
```

```
MVR6 Multicast VLAN: 111
MVR6 Source-address: fe80::111
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 64
SwitchA# show mvr6 groups
VLAN  Interface  Group Address                Uptime     Expire-time
10       eth-0-2     ff0e::1234                 00:03:23   00:02:03
10       eth-0-2     ff0e::1235                 00:03:23   00:02:03
10       eth-0-2     ff0e::1236                 00:03:23   00:02:03
10       eth-0-2     ff0e::1237                 00:03:23   00:02:03
10       eth-0-2     ff0e::1238                 00:03:23   00:02:03
10       eth-0-2     ff0e::1239                 00:03:23   00:02:03
……
10       eth-0-2     ff0e::1273                 00:03:23   00:02:03
```

14 RPC API Configuration Guide

14.1 Management Configuration

14.1.1 Introduction

RPC API allows users to remotely control switches via software, which currently supports JSON-RPC over HTTP and HTTP basic authentication.

14.1.2 Configure RPC API

Users can enable RPC API service following the steps below with port 80 by default.

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# service rpc-api enable port 80	Enable RPC API service, and use port TCP 80 (HTTP)
Switch(config)# exit	Exit configuration mode

Users can disable RPC API server following the steps below:

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# service rpc-api disable	Disable RPC API service
Switch(config)# exit	Exit configuration mode

14.1.3 Configure HTTP Authentication for RPC API Service

Users can configure HTTP authentication for RPC API server.

Currently, only HTTP Basic authentication is supported. 401 status code will be returned in the case of authentication failure.

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# username centec password centec	Configure switch username (centec) and password (centec), which can be used for HTTP authentication
Switch(config)# service rpc-api auth-mode basic	Enable HTTP basic authentication for RPC API service
Switch(config)# exit	Exit configuration mode

Cancel HTTP authentication:

Switch1

Switch# configure terminal	Enter configuration mode
Switch(config)# no service rpc-api auth-mode	Disable HTTP authentication for RPC API service
Switch(config)# exit	Exit configuration mode

NOTE

After enabling or disabling HTTP authentication, users must manually restart RPC API service or reboot switch to validate the configurations.

After RPC API is enabled, two imish resources will be occupied for giving commands. In the case of show users, the idle time that RPC API occupies imish remains 0.

14.1.4 Show RPC API Service Information

Show current RPC API configuration

Switch1

Switch# show services rpc-api	Show current RPC API service configuration

RPC API services configuration:

HTTP server: running, port: 80, authentication mode: none

14.2 RPC API Specification

14.2.1 Overview

RPC API services are subject to standard JSON-RPC specification. You can execute CLI command lines of switches via JSON RPC method: 'executeCmds'. The initial mode is privilege EXEC (#) mode by default.

Users should send JSON-RPC (over HTTP) to request URL: ***Http://<switch management port IP address>:<port number>/command-api***, and the requested and returned JSON-RPC formats are as below:

14.2.2 JSON-RPC Request

```
{
  "params":[                              command parameter
    {
      "format":"text",                      expected command rollback format, 'text' or' json' , 'text' by default
      "version":1,                          command version number
      "cmds":[                              command list
        "show run",                         command line 1
        "config t",                         command line 2
        "vlan database",                    command line 3
        "vlan 1-8",                         command line 4
        "interface eth-0-1",                command line 5
        "switchport mode trunk",            command line 6
        "switchport trunk allowed vlan add 2",    command line 7
        "shutdown",                         command line 8
        "end",                              command line 9
        "show interface switchport"         command line 10
      ]
    }
  ],
  "jsonrpc":"2.0",                          JSON RPC protocol version number
  "method":"executeCmds",                   method of running switch CLI command
  "id":"70853aff-af77-420e-8f3c-fa9430733a19"   UID in JSON RPC protocol UID
}
```

14.2.3 JSON-RPC Response

```
{
  "jsonrpc":"2.0",                          JSON RPC protocol version number
  "id":"70853aff-af77-420e-8f3c-fa9430733a19",    UID in JSON RPC
  "result":[                                JSON RPC return value list
    {
      "sourceDetails":"version 5.1.6.fcs\n!\n …",    return value of command line 1.
                                            In the case of running success, the original text is output
in "sourceDetails" attribute.
      "errorCode":-1003,                    Error will be output in
      "errorDesc":"unsupported command…",   warnings/errorCode/errorDesc attribute.
"warnings":"% Invalid …",
                                            JSON formatting objects also will be output here.
```

```
    },
    { },                                    return value of command line 2.
    { },                                    return value of command line 3.
    { },                                    return value of command line 4.
    { },                                    return value of command line 5.
    { },                                    return value of command line 6.
    { },                                    return value of command line 7.
    { },                                    return value of command line 8.
    { },                                    return value of command line 9.
    {
      "sourceDetails":" Interface name        : eth-0-1\n Switchport mode       : trunk\n …\n"
    }                                       return value of command line 10.
  ]
}
```

14.2.4 Sample Python Client Codes

Sample pyjsonrpc codes are as below:

```
import pyjsonrpc
import json
http_client = pyjsonrpc.HttpClient(
  url = "http://10.10.39.64:80/command-api",
  username = "centec",
  password = "centec"
)
cmds = {}
cmd_list = ["show run", "config t", "vlan database", "vlan 1-8", "interface eth-0-1", "switchport mode trunk", "switchport trunk
allowed vlan add 2", "shutdown", "end", "show interface switchport"]
cmds['cmds'] = cmd_list
cmds['format'] = 'text'
cmds['version'] = 1
try:
  response = http_client.call("executeCmds", cmds)
  print("json response:");
  json_result = json.dumps(response, indent=4)
  print(json_result)
except Exception, e:
  if e.code == 401:
    print "Unauthorized user"
  else:
    print e.message
    print e.data
```

14.2.5 JSON-RPC Error Codes

JSON-RPC 2.0 error codes are listed below:

Error code:	Description
-32700	JSON-RPC parse error
-32600	Invalid request

-32601	Invalid method
-32602	Invalid parameter
-32603	Internal error

14.2.6 RPC-API Error Codes

RPC-API error codes are listed below:

Error code:	Description
-1000	General error
-2001	Non-supported JSON RPC API version
-2002	JSON RPC must assign ‘params’ and ‘cmds’
-2003	Non-supported JSON response format
-3001	Command execution error: Timeout
-3002	Command execution error: No support the command
-3003	Command execution error: Unauthorized command
-3004	Command execution error: Could not found the command
-3005	Command execution error: Could not convert to JSON format
-3006	Command execution error: Insufficient command line count
-3007	Command execution error: Excessive command line count

15 VPN Configuration Guide

15.1 VRF Configuration

15.1.1 Introduction

Short for VPN virtual routing and forwarding, and also called VPN-instance, VRF is a dedicated entity constructed and maintained by PE for direct connection points. Each VPN-instance contains routing and forwarding tables of one or more CEs in direct connection with the PE. VRF can logically divide one router into multiple virtual routers. Each virtual router works as an individual router, and has its own routing table and corresponding interfaces involving in data forwarding. The virtual routers are independent from each other in business. This fundamentally solves the problem that multiple services operate on one physical device and isolation is needed, which saves user investment in devices and communication resources.

15.1.2 Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# ip vrf vpn1	Create VRF, and enter VRF configuration mode
Switch(config-vrf)# rd 100:1	Create RD. RD may be a combination of one AS number and a digit (xxx:y) or of one IP address and a digit (A.B.C.D:y)
Switch(config-vrf)# router-id 1.1.1.1	Set router tag
Switch(config-vrf)# route-target both 100:1	Create RT. RD may be a combination of one AS number and a digit (xxx:y) or of one IP address and a digit (A.B.C.D:y)
Switch(config-vrf)# import map route-map	Set routing policy for VRF
Switch(config-vrf)# interface eth-0-1	Enter interface mode
Switch(config-if)# no shutdown	Interface up
Switch(config-if)# no switch	Set the interface as layer3 interface
Switch(config-if)# ip vrf forwarding vpn1	Add the interface under VRP vpn1
Switch(config-if)# ip add 1.1.1.1/24	Set IP address
Switch(config-if)# end	Exit interface mode

Switch# show ip vrf vpn1	Show configuration details

15.1.3 Command Validation

Configuration validation via command "**show ip vrf**" will result in the screen echo as below.

```
Switch# show ip vrf
VRF vpn1, FIB ID 1
Router ID: 1.1.1.1 (config)
Interfaces:
  eth-0-1
DUT1# show ip vrf interfaces vpn1
Interface            IP-Address      VRF                Protocol
eth-0-1              1.1.1.1         vpn1               up
Switch# show ip vrf bgp brief
Name                  Default RD          Interfaces
vpn1                  100:1               eth-0-1
Switch# show ip vrf bgp detail
VRF vpn1; default RD 100:1
Interfaces:
  eth-0-1
VRF Table ID = 1
Export VPN route-target communities
  RT:100:1
Import VPN route-target communities
  RT:100:1
import-map: route-map
No export route-map
```

15.2 IPv4 over IPv4 GRE Tunneling Configuration

15.2.1 Introduction

Tunneling is an encapsulation technology of utilizing a network protocol to transmit another network protocol. Specifically, a network protocol encapsulates a data packet of another network protocol in its data packet and transmit it in the network. The path of transmitting encapsulated data packets in the network is called tunnel. Tunnel is a virtual point-to-point link, data packet encapsulation and de-encapsulation must be performed on the two ends of a tunnel. Tunneling refers to a whole process consisting of data encapsulating, transmitting and de-encapsulating.

In the event that two isolated IPv4 networks need to intercommunicate with each other, a tunneling mechanism is needed between the two networks. The gre tunnel linking two isolated IPv4 islands on IPv4 network is called IPv4 gre tunnel, via which an IPv4 message is encapsulated in an IPv4 message via gre protocol to realize transparent transmission of IPv4 message.6 data packets. Gre tunnel protocol will add a gre header containing optional information such as key, sequence and checksum while encapsulating IPv4 messages. To realize a gre tunnel, IPv4 dual-stack protocol must be enabled on the border switch between IPv4 network and IPv6 network.

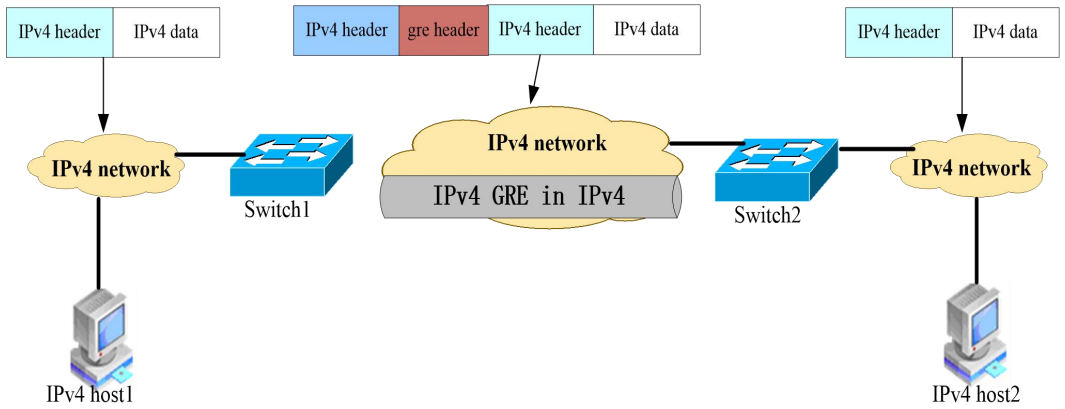


Figure 15-1: Schematic Figure of IPv4 gre over IPv4 Tunnel

IPv4 gre over IPv4 tunnel processes data packets as below:

A device in IPv4 network sends an IPv6 message to the source device Switch 1 of the tunnel.

Switch 1, after determining that the message must be forwarded via the tunnel based on the routing table, encapsulates the IPv4 message with a gre header first and with an outer IPv4 message header, and forwards it out via the physical interface of the tunnel.

The encapsulated message passes through the tunnel and reaches the destination device Switch2, and Switch2 de-encapsulates the message after judging the message destination is a local device.

Switch2 forwards the IPv4 message according to the destination address of the de-encapsulated IPv4 message. If Switch2 exactly is the destination, it forwards the IPv4 message to an upper layer protocol for processing. In the process of de-encapsulating, the key option in the gre header will be checked, and the IPv4 message will be processed only if the key is matched. Otherwise, it will be discarded.

The advantage of this technology is that once the border device of IPv4/IPv4 network realizes the tunnel function, it can perform transparent message transmission from one end to another end for message check, which can make full use of the existing IPv4 network investment.

I. IPv4 GRE tunnel

The source and destination addresses of GRE tunnel are manually specified, and the tunnel provides point-to-point connection. GRE tunnel can be constructed between two border routers to provide stable connection for IPv4 networks separated by IPv4, or between the terminal system and border router to provide the terminal system access to IPv4 networks.

GRE tunnel requires to manually specify the source address and destination address, and gre key configuration is optional.

15.2.2 Configure IPv4 GRE tunnel

I. Topology

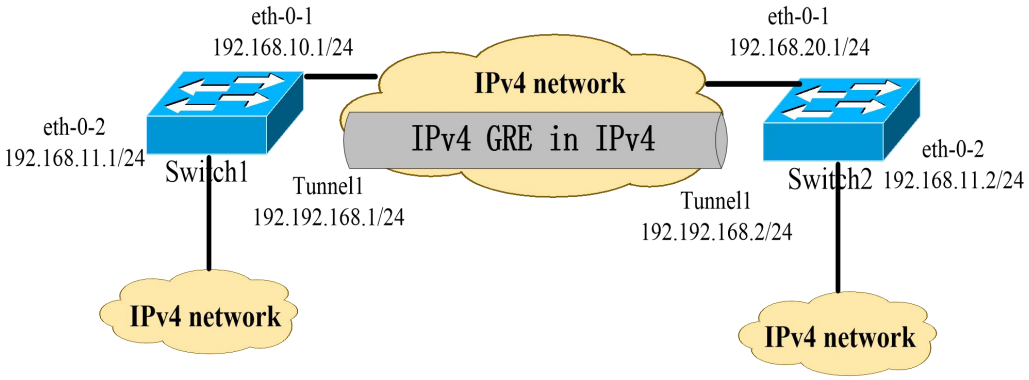


Figure 15-2: Configure IPv4 GRE tunnel

As shown in the figure above, two IPv4 networks are connected with the middle IPv4 network via Switch1 and Switch2 respectively, wherein it is required to construct an IPv4 gre tunnel between Switch1 and Switch2 to realize intercommunication between the two IPv4 networks.

II. Configuration

Switch1

Configure IPv4 address, to realize layer 3 packet reachability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 192.168.10.1/24	Configure interface IPv4 address
Switch(config)# ip route 192.168.20.0/24 192.168.10.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 192.168.10.2 0.0.2222	Configure static ARP, 0.0.2222 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

Configure eth-0-2 IPv6 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ip address 192.168.11.1/24	Configure interface IPv4 address

Configure tunnel1 Interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel mode gre	Configure tunnel mode as gre
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel destination 192.168.20.1	Configure tunnel destination
Switch(config-if)# tunnel gre key 100	Configure tunnel gre key as 100
Switch(config-if)# ip address192.192.168.1/24	Configure tunnel interface IPv4 address

Configure tunnel keepalive function

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Enter tunnel1 interface mode
Switch(config-if)# keepalive 5 3	Enable tunnel1 keepalive function

Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

Configure static IPv4 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip route 3.3.3.3/24 tunnel1	Configure static routing for reaching the opposite end

Switch2

Configure IPv4 address, to realize layer 3 packet reachability

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-1 as layer 3 routed port
Switch(config-if)# ip address 192.168.20.1/24	Configure interface IPv4 address

Switch(config)# ip route 192.168.10.0/24 192.168.20.2	Configure IPv4 static routing for reaching the opposite end
Switch(config)# arp 192.168.20.2 0.0.1111	Configure static ARP, 0.0.1111 as the next hop system MAC address. (The ARP entry also can be obtained via dynamic learning)

Configure eth-0-2 IPv4 address

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Configure eth-0-2 as layer 3 routed port
Switch(config-if)# ip address 192.168.11.2/24	Configure interface IPv4 address

Configure tunnel1 Interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Create tunnel virtual interface
Switch(config-if)# tunnel mode gre	Configure tunnel mode as gre
Switch(config-if)# tunnel source eth-0-1	Set eth-0-1 as tunnel source
Switch(config-if)# tunnel destination 192.168.10.1	Configure tunnel destination
Switch(config-if)# tunnel gre key 100	Configure tunnel gre key as 100
Switch(config-if)# ip address192.192.168.2/24	Configure tunnel interface IPv4 address

Configure tunnel keepalive function

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface tunnel1	Enter tunnel1 interface mode
Switch(config-if)# keepalive 5 3	Enable tunnel1 keepalive function

Configure tunnel decap interface

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# tunnel enable	Set eth-0-1 as tunnel decap

6) Configure static IPv4 routing for reaching the opposite end

Switch# configure terminal	Enter global configuration mode
Switch(config)# ip route 4.4.4.4/24 tunnel1	Configure static routing for reaching the opposite end

III. Check configuration result

Switch1

```
Switch1# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Internet primary address:
    192.192.168.1/24 pointopoint 192.192.168.255
  Tunnel protocol/transport GRE/IP, Status Valid
  Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
  Tunnel DSCP inherit,  Tunnel TTL 255
  Tunnel GRE key enable: 100
  Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
  0 packets input, 0 bytes
  0 packets output, 0 bytes
```

Switch2

```
Switch2# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Internet primary address:
    192.192.168.2/24 pointopoint 192.192.168.255
  Tunnel protocol/transport GRE/IP, Status Valid
  Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
  Tunnel DSCP inherit,  Tunnel TTL 255
  Tunnel GRE key enable: 100
  Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
  0 packets input, 0 bytes
  0 packets output, 0 bytes
```

NOTE

Settings must be made to realize layer 3 routability of IPv4 message, otherwise tunnel message forwarding will fail.

Tunnel interface must be configured IPv4 address, otherwise the router configured on the interface is inactive.

16 Reliability Configuration Guide

16.1 BHM Configuration

16.1.1 Introduction

BHM is a module for monitoring other protocol processes. If a monitored process gives no response for a long time (30 seconds), BHM module will take actions or prompt users to restore the system. The aforementioned actions include printing warning message on the terminal, shutting down all ports, or rebooting system. The actions are configurable, and the default action is rebooting system.

The protocol modules monitored by BHM include: RIP, RIPNG, OSPF, OSPF6, BGP, LDP, RSVP, PIM, PIM6, 802.1X, LACP, MSTP, DHCP-RELAY, DHCP-RELAY6, RMON, OAM, ONM, SSH, SNMP, PTP, SSM, as well as some system processes (NSM, MI, CHSM, HSRVD).

16.1.2 Terms

BHM: Beat heart Monitor

16.1.3 Configuration

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# sysmon enable	Enable system monitoring function
Switch1(config)# heart-beat-monitor enable	Enable BHM module function
Switch1(config)# heart-beat-monitor reactivate reload system	Configure monitoring measure as “rebooting system”

16.1.4 Command Validation

Show the configuration result by running the following command.

Switch1# show heart-beat-monitor

heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.

16.2 CFM Configuration

This chapter presents a complete instance of connectivity fault management (CFM) configuration. For detailed information on command usage in the instance, please see the CFM command reference. To prevent repetition, the CFM command reference doesn't include the common commands.

16.2.1 Introduction

CFM can detect, verify, locate and notify linkage fault in the Ethernet network in accordance with 802.1ag protocol. CFM also can identify and verify Ethernet paths. CFM is a part of operation administration and maintenance module (OAM). CFM is transparent to user data message and can identify connectivity fault to the utmost extent.

CFM uses standard Ethernet message, only different from Ethernet protocol type. The supported CFM messages include:

- Continuity check (CC) message

  Continuity check messages are sent periodically to enable endpoints MEP and intermediate nodes MIP of the maintenance domain to discover other MEPs. It is used to detect loss of continuity (LOC) between any pair of MEPs.

- Ethernet loopback (LB) message

  MEP sends an LB message to verify whether the other MEP or MIP is reachable. LB message is similar to Internet control message protocol (ICMP) ping message.

- Ethernet link trace (LT) message

  MEP sends LT messages to trace the MIP of every hop towards a destination MEP/MIP. LT message is similar to UDP link trace message.

- Ethernet frame delay (DM) message

ETH-DM can be used for OAM-on-demand to measure frame delay and frame delay variation. The measurement of frame delay and frame delay variation is completed by periodically sending frames with ETH-DM information to the peer MEP and receiving frames with ETH-DM information from the peer MEP at the diagnostic interval. Every MEP can measure frame delay and frame delay variation.

An MEP periodically sends frames with ETH-DM information to its peer MEP within the same ME when it can generate frames with ETH-DM information. An MEP expects to receive frames with ETH-DM information within the same ME when it generates frames with ETH-DM information.

- Ethernet locking signal (LCK) message

  The Ethernet locking signal (ETH-LCK) function is for notifying administrative locking of the server layer (sublayer) MEP and subsequent data traffic flow interruption. The traffic is sent to the MEP that expects to receive it. It enables the MEP receiving frames with ETH-LCK information to tell fault or administrative locking of the server layer (sublayer) MEP.

- Ethernet client signal failure (CSF)

  The Ethernet client signal failure function refers to that the server MEP notifies the detected failure or error to the corresponding server MEP, and the opposite server MEP notifies such failure or error to the opposite client MEP. It generally applies if the client MEP is unable to notify the opposite MEP, where CC or AIS is not available. CSF message

is sent by the server MEP to the opposite server MEP. CSF is applied in point-to-point Ethernet transmission only.

- Ethernet frame frame loss measurement (LM) message

  ETH-LM is used for gathering the numerical values of counter, and applied to ingress and egress service frames where the counter keeps the count of the sent and received data frames between a pair of MEPs.

  ETH-LM is realized by sending frames with ETH-LM information to its peer MEP and receiving frames with ETH-LM information from the peer MEP similarly.

16.2.2 References

IEEE 802.1ag/D8.1

16.2.3 Limit

CFM functionally conflicts with 802.1x and mirror destination, so they

should not be configured together on the same port;

16.2.4 Configure CC/LB/LT/AIS/DM

I. Topology

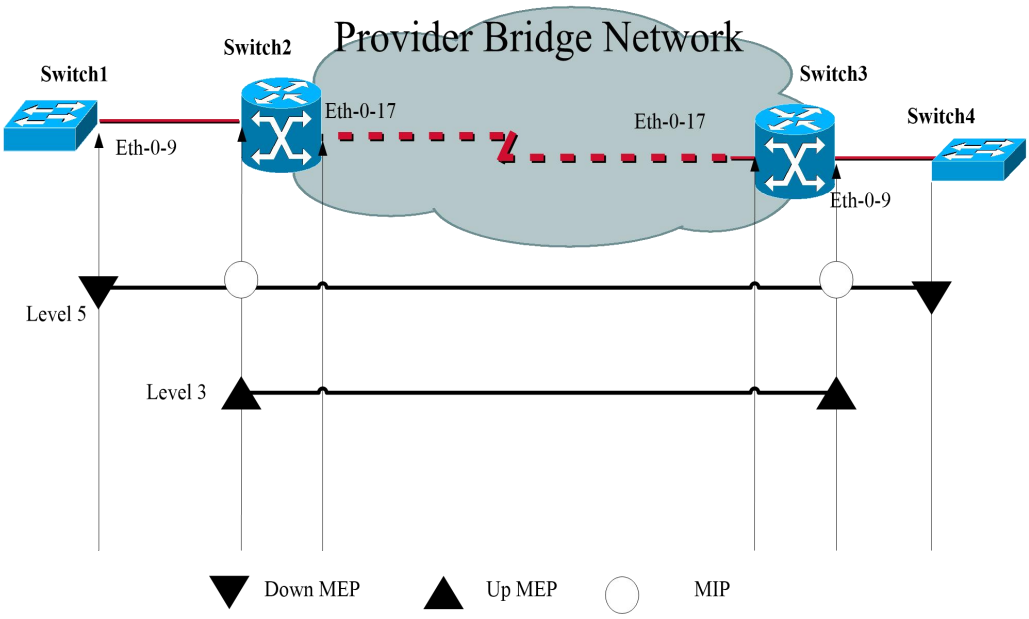


Figure 16-1 CFM Topology

II. Configuration

Switch 1

Switch1# configure terminal	Enter global configuration mode
Switch1 (config)# vlan database	Enter VLAN configuration mode

Switch1(config vlan)# vlan 30	Create VLAN 30
Switch1(config vlan)# exit	Exit VLAN configuration mode
Switch1(config)# ethernet cfm enable	Globally enable CFM
Switch1(config)# ethernet cfm mode y1731	Configure CFM mode
Switch1(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch1(config-ether-cfm)# service cst vlan 30	Create service cst
Switch1(config-ether-cfm)# exit	Exit CFM configuration mode
Switch1(config)# interface eth-0-9	Enter port mode
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	Create maintenance domain endpoint
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	Create maintenance domain remote node, mac as remote mep mac
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	Enable connectivity check of service cst of maintenance domain cust
Switch1(config)# ethernet cfm ais suppress alarm enable domain cust vlan 30	Set to suppress other loc errors if alarm indication signal ais and loc error is detected
Switch1 (config)# end	Exit global configuration mode

Switch 2

Switch2# configure terminal	Enter global configuration mode
Switch2 (config)# vlan database	Enter VLAN configuration mode
Switch2 (config-vlan)# vlan 30	Create VLAN 30
Switch2(config-vlan)# exit	Exit VLAN configuration mode
Switch2(config)# ethernet cfm enable	Globally enable CFM
Switch2(config)# ethernet cfm mode y1731	Configure CFM mode

Switch2(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch2(config-ether-cfm)# service cst vlan 30	Create service cst
Switch2(config-ether-cfm)# exit	Exit CFM configuration mode
Switch2(config)# ethernet cfm domain provid level 3	Create maintenance domain provid
Switch2(config-ether-cfm)# service cst vlan 30	Create service cst
Switch2(config-ether-cfm)# exit	Exit CFM configuration mode
Switch2(config)# interface eth-0-9	Enter port mode
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch2(config-if)# ethernet cfm mip level 5 vlan 30	Create maintenance domain intermediate node
Switch2(config-if)# ethernet cfm mep up mpid 666 domain provid vlan 30 interval 1	Create maintenance domain endpoint
Switch2(config-if)# ethernet cfm mep crosscheck mpid 999 domain provid vlan 30 mac 6a08.051e.bd09	Create maintenance domain remote node, mac as remote mep mac
Switch2(config-if)# ethernet cfm ais status enable all domain provid vlan 30 level 5 multicast	Enable ais
Switch2(config-if)# ethernet cfm server-ais status enable level 5 interval 1	Configure ais server
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-17	Enter port mode
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# ethernet cfm cc enable domain provid vlan 30	Enable connectivity check of service cst of maintenance domain provid

Switch2 (config)# end	Exit global configuration mode

Switch3

Switch3# configure terminal	Enter global configuration mode
Switch3 (config)# vlan database	Enter VLAN configuration mode
Switch3 (config-vlan)# vlan 30	Create VLAN 30
Switch3(config-vlan)# exit	Exit VLAN configuration mode
Switch3(config)# ethernet cfm enable	Globally enable CFM
Switch3(config)# ethernet cfm mode y1731	Configure CFM mode
Switch3(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch3(config-ether-cfm)# service cst vlan 30	Create service cst
Switch3(config-ether-cfm)# exit	Exit CFM configuration mode
Switch3(config)# ethernet cfm domain provid level 3	Create maintenance domain provid
Switch3(config-ether-cfm)# service cst vlan 30	Create service cst
Switch3(config-ether-cfm)# exit	Exit CFM configuration mode
Switch3(config)# interface eth-0-9	Enter port mode
Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch3(config-if)# ethernet cfm mip level 5 vlan 30	Create maintenance domain intermediate node
Switch3(config-if)# ethernet cfm mep up mpid 999 domain provid vlan 30 interval 1	Create maintenance domain endpoint
Switch3(config-if)# ethernet cfm mep crosscheck mpid 666 domain provid vlan 30 mac 0e1d.a7d7.fb09	Create maintenance domain remote node, mac as remote mep mac
Switch3(config-if)# no shutdown	Open the interface
Switch3(config-if)# exit	Exit interface mode
Switch3(config)# interface eth-0-17	Enter port mode

Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch3(config-if)# no shutdown	Open the interface
Switch3(config-if)# exit	Exit interface mode
Switch3(config)# ethernet cfm cc enable domain provid vlan 30	Enable connectivity check of service cst of maintenance domain provid
Switch3 (config)# end	Exit global configuration mode

Switch4

Switch4# configure terminal	Enter global configuration mode
Switch4 (config)# vlan database	Enter VLAN configuration mode
Switch4(config vlan)# vlan 30	Create VLAN 30
Switch4(config vlan)# exit	Exit VLAN configuration mode
Switch4(config)# ethernet cfm enable	Globally enable CFM
Switch4(config)# ethernet cfm mode y1731	Configure CFM mode
Switch4(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch4(config-ether-cfm)# service cst vlan 30	Create service cst
Switch4(config-ether-cfm)# exit	Exit CFM configuration mode
Switch4(config)# interface eth-0-9	Enter port mode
Switch4(config-if)# switchport mode trunk	Configure the port as trunk
Switch4(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch4(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	Create maintenance domain endpoint
Switch4(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	Create maintenance domain remote node, mac as remote mep mac
Switch4(config-if)# no shutdown	Open the interface
Switch4(config-if)# exit	Exit interface mode
Switch4(config)# ethernet cfm cc enable domain cust vlan 30	Enable connectivity check of service cst of maintenance domain cust

Switch4 (config)# end	Exit global configuration mode

Ⅲ.Command validation

Check MEP and MIP

The following commands can be run to view related information of MEP and MIP on Switch1 and Switch2.

Switch1# show ethernet cfm maintenance-points

```
######Local MEP:
MPID Direction DOMAIN LEVEL TYPE VLAN PORT     CC-Status Mac-address    RDI  Interval
--------------------------------------------------------------------------------
66   Down MEP   cust   5     MEP  30   eth-0-9  enabled   fa02.cdff.6a09 True 3.33ms
######Local MIP:
Level   VID  TYPE    PORT          MAC
------------------------------------------------------------
######Remote MEP:
MPID  LEVEL VLAN ACTIVE Remote Mac     RDI   FLAGS    STATE
------------------------------------------------------------
99    5     30   Yes    d036.4567.8009 True  Learnt    UP
```

Switch2# show ethernet cfm maintenance-points

```
######Local MEP:
MPID Direction DOMAIN LEVEL TYPE VLAN PORT     CC-Status Mac-address    RDI
------------------------------------------------------------------------------
666  Up MEP    provid 3     MEP  30   eth-0-9  enabled   0e1d.a7d7.fb09 False
######Local MIP:
Level   VID  TYPE    PORT          MAC
------------------------------------------------------------
5       30    MIP     eth-0-9       0e1d.a7d7.fb09
######Remote MEP:
MPID  LEVEL VLAN ACTIVE Remote Mac     RDI   FLAGS     STATE
------------------------------------------------------------
999   3     30    Yes    6a08.051e.bd09  True  Learnt    UP
```

Ethernet Loopback Check

The following commands are run for looping back remote MEP according to remote MEP addresses.

```
Switch1# ethernet cfm loopback mac d036.4567.8009 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ------------------------------------
Success rate is 100 percent(1/1)
```

The following commands are run for looping back remote MEP according to multicast addresses.

```
Switch1# ethernet cfm loopback multicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
Host MEP: 66
Number of RMEPs that replied to mcast frame = 1
LBR received from the following
 9667.bb68.f308
 success rate is  100 (1/1)
```

The following commands are run for looping back remote MEP according to remote MEP identification.

```
Switch1# ethernet cfm loopback unicast rmepid 99 mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ------------------------------------
 Success rate is 100 percent(1/1)
```

The following commands are run for looping back remote MIP according to remote MIP addresses.

```
Switch1# ethernet cfm loopback mac 0e1d.a7d7.fb09 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ------------------------------------
 Success rate is 100 percent(1/1)
```

Check Remote Fault Indication RDI

The following commands are run for showing RDI information.

```
Switch1# show ethernet cfm maintenance-points local mep domain cust
MPID Direction DOMAIN LEVEL TYPE VLAN PORT    CC-Status Mac-address    RDI Interval
--------------------------------------------------------------------------------
66   Down MEP  cust   5  MEP  30   eth-0-9  enabled   fa02.cdff.6a09 True 3.33ms
```

Error Check

The error information before clearing of local MEP errors is as below.

```
Switch1# show ethernet cfm errors domain cust
Level Vlan MPID RemoteMac      Reason                        ServiceId
5     30   66  d036.4567.8009 errorCCMdefect: rmep not found      cst
5     30   66  d036.4567.8009 errorCCMdefect: rmep not found clear cst
Time
2011/05/27 3:19:18
2011/05/27 3:19:32
```

The following command is run for clearing error information.

```
Switch1# clear ethernet cfm errors domain cust
```

The error information after clearing of local MEP errors is as below.

```
Switch1# clear ethernet cfm errors domain cust
Level Vlan MPID RemoteMac      Reason                    ServiceId
```

Check AIS

The following command is run for disabling connectivity check on Switch1.

```
Switch1(config)# no ethernet cfm cc enable domain cust vlan 30
```

The following command is running for disabling connectivity check on Switch3.

```
Switch3(config)# no ethernet cfm cc enable domain cust vlan 30
```

The following command is run for checking the ais status on Switch2.

```
Switch2# show ethernet cfm ais mep 666 domain cust vlan 30
AIS-Status: Enabled
AIS Period: 1
Level to transmit AIS: 7
AIS Condition: No
-------------------------------------------------------
  Configured defect condition    detected(yes/no)
-------------------------------------------------------
  unexpected-period              no
  unexpected-MEG level           no
  unexpected-MEP                 no
  Mismerge                       no
  LOC                       yes
```

The following command is run for checking the ais status of Switch1.

```
Switch1# show ethernet cfm ais mep 66 domain cust vlan 30
AIS-Status: Disabled
AIS Condition: Yes
```

Check LinkTrace

The following command is run for tracing remote MEP according to remote MEP addresses.

```
Switch1# ethernet cfm linktrace mac d036.4567.8009 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
-------------------------------
Received Hops: 1
-------------------------------
TTL                 : 63
Fowarded            : True
Terminal MEP        : False
Relay Action        : Rly FDB
Ingress Action      : IngOk
Ingress MAC address : 0e1d.a7d7.fb09
Ingress Port ID Type : ifName
Ingress Port ID     : eth-0-9
-------------------------------
Received Hops: 2
-------------------------------
TTL                 : 62
```

```
Fowarded                : True
Terminal MEP            : False
Relay Action            : Rly FDB
Egress Action           : EgrOk
Egress MAC address      : 6a08.051e.bd09
Egress Port ID Type     : ifName
Egress Port ID          : eth-0-9
--------------------------------
Received Hops: 3
--------------------------------
TTL                     : 61
Fowarded                : False
Terminal MEP            : True
Relay Action            : Rly Hit
Ingress Action          : IngOk
Ingress MAC address     : d036.4567.8009
Ingress Port ID Type    : ifName
Ingress Port ID         : eth-0-9
```

The following command is run for tracing remote MEP according to remote MEP identification.

```
Switch1# ethernet cfm linktrace rmepid 99 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
--------------------------------
Received Hops: 1
--------------------------------
TTL                 : 63
Fowarded                : True
Terminal MEP            : False
Relay Action            : Rly FDB
Ingress Action          : IngOk
Ingress MAC address     : 0e1d.a7d7.fb09
Ingress Port ID Type    : ifName
Ingress Port ID     : eth-0-9
--------------------------------
Received Hops: 2
--------------------------------
TTL                     : 62
Fowarded                : True
Terminal MEP            : False
Relay Action            : Rly FDB
Egress Action           : EgrOk
Egress MAC address      : 6a08.051e.bd09
Egress Port ID Type     : ifName
Egress Port ID          : eth-0-9
--------------------------------
Received Hops: 3
--------------------------------
TTL                     : 61
Fowarded                : False
Terminal MEP            : True
Relay Action            : Rly Hit
Ingress Action          : IngOk
```

```
Ingress MAC address      : d036.4567.8009
Ingress Port ID Type     : ifName
Ingress Port ID          : eth-0-9
```

The following command is run for tracing remote MIP according to remote MIP addresses.

```
Switch1# ethernet cfm linktrace 6a08.051e.bd09 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
------------------------------
Received Hops: 1
------------------------------
TTL                      : 63
Fowarded                 : True
Terminal MEP             : False
Relay Action             : Rly FDB
Ingress Action           : IngOk
Ingress MAC address      : 0e1d.a7d7.fb09
Ingress Port ID Type     : ifName
Ingress Port ID          : eth-0-9
------------------------------
Received Hops: 2
------------------------------
TTL                      : 62
Fowarded                 : False
Terminal MEP             : False
Relay Action             : Rly Hit
Egress Action            : EgrOk
Egress MAC address       : 6a08.051e.bd09
Egress Port ID Type      : ifName
Egress Port ID           : eth-0-9
```

Frame Delay Measurement Check

The following command is run for measuring both-way delay and delay variation.

```
Switch1# ethernet cfm dmm  rmepid 99 mepid 66 count 5 domain cust vlan 30
   Delay measurement statistics:
   DMM Packets transmitted       : 5
   Valid DMR packets received    : 5
   Index     Two-way delay     Two-way delay variation
      1        4288 usec                0 usec
      2        4312 usec               24 usec
      3        4296 usec               16 usec
      4        4320 usec               24 usec
      5        4264 usec               56 usec
   Average delay              : 4296 usec
   Average delay variation    : 24 usec
   Best case delay            : 4264 usec
   Worst case delay           : 4320 usec
```

Before enabling one-way delay measurement, clock synchronization must be set. The following command is run for enabling one-way delay measurement on Switch1.

```
Switch1#ethernet cfm 1dm rmepid 99 mepid 66 count 5 domain cust vlan 30
```

The following command is run for showing the result of one-way delay measurement on Switch4:

```
Switch4# show ethernet cfm delaymeasurement cache
  Remote MEP      : 66
  Remote MEP vlan  : 30
  Remote MEP level : 5
  DMM Packets transmitted              : 0
  Valid DMR packets received           : 0
  Valid 1DM packets received           : 5
  Index  One-way delay  One-way delay variation  Received Time
    1    16832 usec              0 usec  2011/07/19 17:27:46
    2    16176 usec            656 usec  2011/07/19 17:27:47
    3    15448 usec            728 usec  2011/07/19 17:27:48
    4    14800 usec            648 usec  2011/07/19 5:27:49 PM
    5    15406 usec            606 usec  2011/07/19 5:27:50 PM
  Average delay               : 15732 usec
  Average delay variation     : 527 usec
  Best case delay             : 14800 usec
  Worst case delay            : 16832 usec
```

16.2.5 Configure LCK

I. Topology

Please refer to 1.3.1.

II. Configuration

Please refer to MD/MA/MEP configuration in Section 1.3.2.

Configure locking on Switch2

Switch 2

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-9	Enter port mode
Switch2(config-if)# ethernet cfm lck enable mep 666 domain provid vlan 30 tx-level 5 interval 1	Configure locking MEP 666, and specify to send locking message to level 5 at an interval of 1 second
Switch2(config-if)# end	Exit interface mode

I. Command validation

The following command is run for showing LCK condition on Switch2：

Switch2# show ethernet cfm lck

```
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
```

```
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
--------------------------------------------------------------------------
MPID Domain      VLAN En Rx-LC Rx-I Tx-Domain    Tx-I
--------------------------------------------------------------------------
666 provid      30   Y N     N/A  cust       1
```

The following command is run for showing LCK condition on Switch1:

Switch1# show ethernet cfm lck

```
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
--------------------------------------------------------------------------
MPID Domain      VLAN En Rx-LC Rx-I Tx-Domain    Tx-I
--------------------------------------------------------------------------
66   cust        30   N Y    1    N/A         N/A
```

16.2.6 Configure CSF

I. Topology

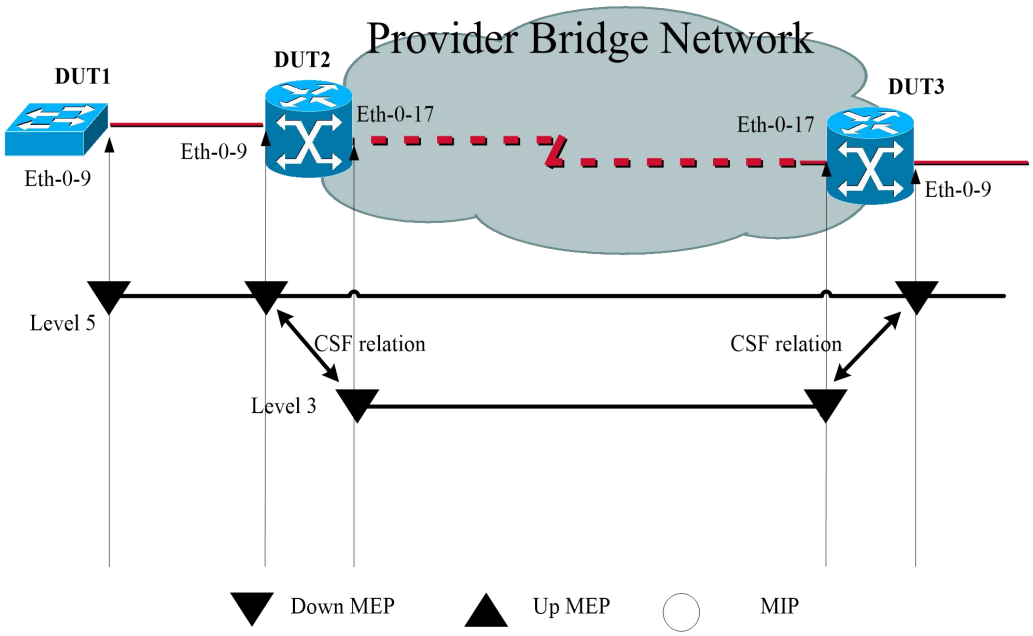


Figure 16-2 CFM CSF Topology

II. Configuration

Switch 1

Switch1# configure terminal	Enter global configuration mode

Switch1 (config)# vlan database	Enter VLAN configuration mode
Switch1(config vlan)# vlan 30	Create VLAN 30
Switch1(config vlan)# exit	Exit VLAN configuration mode
Switch1(config)# ethernet cfm enable	Globally enable CFM
Switch1(config)# ethernet cfm mode y1731	Configure CFM mode
Switch1(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch1(config-ether-cfm)# service cst vlan 30	Create service cst
Switch1(config-ether-cfm)# exit	Exit CFM configuration mode
Switch1(config)# interface eth-0-9	Enter port mode
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	Create maintenance domain endpoint
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	Create maintenance domain remote node, mac as remote mep mac
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	Enable connectivity check of service cst of maintenance domain cust
Switch1 (config)# end	Exit global configuration mode

Switch 2

Switch2# configure terminal	Enter global configuration mode
Switch2 (config)# vlan database	Enter VLAN configuration mode
Switch2(config vlan)# vlan 20,30	Create VLAN 20,30
Switch2(config vlan)# exit	Exit VLAN configuration mode
Switch2(config)# ethernet cfm enable	Globally enable CFM
Switch2(config)# ethernet cfm mode y1731	Configure CFM mode
Switch2(config)# ethernet cfm domain cust	Create maintenance domain cust

level 5	
Switch2(config-ether-cfm)# service cst vlan 30	Create service cst
Switch2(config)# ethernet cfm domain provid level 3	Create maintenance domain provid
Switch2(config-ether-cfm)# service cst vlan 20	Create service cst
Switch2(config-ether-cfm)# exit	Exit CFM configuration mode
Switch2(config)# interface eth-0-9	Enter port mode
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch2(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	Create maintenance domain endpoint
Switch2(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	Create maintenance domain remote node, mac as remote mep mac
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-17	Enter port mode
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan add 20	Configure the port to allow vlan 20
Switch2 (config-if)# ethernet cfm mep down mpid 666 domain provid vlan 20 interval 1	Create maintenance domain endpoint
Switch2(config-if)# no shutdown	Open the interface
Switch2(config)# ethernet cfm cc enable domain cust vlan 30	Enable connectivity check of service cst of maintenance domain cust
DUT (config)# ethernet cfm csf client domain cust vlan 30 mepid 99 server domain provid vlan 20 mepid 666 interval 1	Configure CSF connection relation
Switch2 (config)# end	Exit global configuration mode

Switch 3

Switch3# configure terminal	Enter global configuration mode

Switch3 (config)# vlan database	Enter VLAN configuration mode
Switch3(config vlan)# vlan 20,30	Create VLAN 20,30
Switch3(config vlan)# exit	Exit VLAN configuration mode
Switch3(config)# ethernet cfm enable	Globally enable CFM
Switch3(config)# ethernet cfm mode y1731	Configure CFM mode
Switch3(config)# ethernet cfm domain cust level 5	Create maintenance domain cust
Switch3(config-ether-cfm)# service cst vlan 30	Create service cst
Switch3(config)# ethernet cfm domain provid level 3	Create maintenance domain provid
Switch3(config-ether-cfm)# service cst vlan 20	Create service cst
Switch3(config-ether-cfm)# exit	Exit CFM configuration mode
Switch3(config)# interface eth-0-9	Enter port mode
Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# switchport trunk allowed vlan add 30	Configure the port to allow vlan 30
Switch3(config-if)# ethernet cfm mep down mpid 88 domain cust vlan 30 interval 1	Create maintenance domain endpoint
Switch3(config-if)# no shutdown	Open the interface
Switch3(config-if)# exit	Exit interface mode
Switch3(config)# interface eth-0-17	Enter port mode
Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# switchport trunk allowed vlan add 20	Configure the port to allow vlan 20
Switch3 (config-if)# ethernet cfm mep down mpid 999 domain provid vlan 20 interval 1	Create maintenance domain endpoint
Switch3(config-if)# no shutdown	Open the interface
Switch3(config)# ethernet cfm cc enable domain cust vlan 30	Enable connectivity check of service cst of maintenance domain cust
Switch3(config)# ethernet cfm csf client domain cust vlan 30 mepid 88 server domain provid vlan 20 mepid 999 interval 1	Configure CSF connection relation
Switch3 (config)# end	Exit global configuration mode

III. Command validation

The following command is run for disabling connectivity check on Switch1, to trigger loc error on Switch2:

```
Switch1(config)# no ethernet cfm cc enable domain cust vlan 30
```

The MEP 99 on Switch2 will report loc, causing MEP 666 to send a CSF message (reason: los):

The following command is run for showing CSF condition on Switch2:

```
Switch2# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
-------------------------------------------------------------------------
Client Mep                  Server Mep
MPID Cli-Domain   VLAN CTR   ECC MPID Srv-Domain   VLAN SRR   Tx-I Rx-I
-------------------------------------------------------------------------
99   cust         30   L     N   666  provid       20   N/A   1    N/A
```

On Switch3, MEP 999 will receive a CSF message and notify it to client MEP 88, and then the client MEP will turn into CSF condition.

The following command is run for showing CSF condition on Switch3:

```
Switch3# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
-------------------------------------------------------------------------
Client Mep                  Server Mep
MPID Cli-Domain   VLAN CTR   ECC MPID Srv-Domain   VLAN SRR   Tx-I Rx-I
-------------------------------------------------------------------------
88   cust         30   N/A   Y   999  provid       20   L     1    1
```

16.2.7 Configure Double-end LM

I. Topology

Please refer to 1.3.1.

II. Configuration

Please refer to MD/MA/MEP configuration in Section 1.3.2.

Enable double-end LM function on Switch1 and Switch4.

Switch 1

Switch1# configure terminal	Enter global configuration mode

Switch1(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 66 all-cos cache-size 10	Configure double-end LM function
Switch1 (config)# end	Exit configuration mode

Switch 4

Switch4# configure terminal	Enter global configuration mode
Switch4(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 99 all-cos cache-size 10	Configure double-end LM function
Switch4 (config)# end	Exit configuration mode

III. Command validation

The following command is run for showing lm result on Switch1:

```
Switch1# show ethernet cfm lm domain cust vlan 30 mepid 66
DOMAIN     : cust
VLAN       : 30
MEPID      : 66
Start Time : 2013/07/16 1:36:56
End Time   : 2013/07/16 1:37:07
Notes      : 1. When the difference of Tx is less than the difference of Rx,
               the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
               ratio should be 100%;
             3. When calculate average loss and loss ratio, invalid or loc nodes
               will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all        0       000.0000%          0       000.0000% 01:36:57
2     all        0       000.0000%          0       000.0000% 01:36:58
3     all        0       000.0000%          0       000.0000% 1:36:59 AM
4     all        0       000.0000%          0       000.0000% 1:37:00 AM
5     all        0       000.0000%          0       000.0000% 1:37:01 AM
6     all        0       000.0000%          0       000.0000% 1:37:02 AM
7     all        0       000.0000%          0       000.0000% 1:37:03 AM
8     all        0       000.0000%          0       000.0000% 1:37:04 AM
9     all        0       000.0000%          0       000.0000% 1:37:05 AM
10    all        0       000.0000%          0       000.0000% 01:37:07
--------------------------------------------------------------------------------
Maximum Local-loss  : 0         Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0         Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0         Average Local-loss Ratio  : 000.0000%
```

```
Maximum Remote-loss : 0          Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0          Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0          Average Remote-loss Ratio : 000.0000%
```

The following command is run for showing lm result on Switch4:

```
Switch4# show ethernet cfm lm domain cust vlan 30 mepid 99
DOMAIN     : cust
VLAN       : 30
MEPID      : 99
Start Time : 2013/07/16 1:37:11 AM
End Time   : 2013/07/16 1:37:22 AM
Notes      : 1. When the difference of Tx is less than the difference of Rx,
               the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
               ratio should be 100%;
             3. When calculate average loss and loss ratio, invalid or loc nodes
               will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all        0       000.0000%          0       000.0000% 1:37:12 AM
2     all        0       000.0000%          0       000.0000% 1:37:13 AM
3     all        0       000.0000%          0       000.0000% 1:37:14 AM
4     all        0       000.0000%          0       000.0000% 1:37:16 AM
5     all        0       000.0000%          0       000.0000% 1:37:17 AM
6     all        0       000.0000%          0       000.0000% 1:37:18 AM
7     all        0       000.0000%          0       000.0000% 1:37:19 AM
8     all        0       000.0000%          0       000.0000% 1:37:20 AM
9     all        0       000.0000%          0       000.0000% 1:37:21 AM
10    all        0       000.0000%          0       000.0000% 1:37:22 AM
--------------------------------------------------------------------------------
Maximum Local-loss  : 0          Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0          Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0          Average Local-loss Ratio  : 000.0000%
Maximum Remote-loss : 0          Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0          Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0          Average Remote-loss Ratio : 000.0000%
```

16.2.8 Configure Single-end LM

I. Topology

Please refer to 1.3.1.

II. Configuration

Please refer to MD/MA/MEP configuration in Section 1.3.2.

Enable single-end LM function on Switch1 and Switch4.

Switch 1

Switch1# configure terminal	Enter global configuration mode

Switch1(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 66 all-cos	Configure single-end LM function
Switch1 (config)# end	Exit configuration mode

Switch 4

Switch4# configure terminal	Enter global configuration mode
Switch4(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 99 all-cos	Configure single-end LM function
Switch4 (config)# end	Exit configuration mode

III. Command validation

The following command is run for sending LMM message from Switch1 and showing lm result:

```
Switch1#  ethernet cfm lm single-ended domain cust vlan 30 rmepid 99 mepid 66 count 10
DOMAIN    : cust
VLAN      : 30
MEPID     : 66
Start Time : 2013/07/16 1:39:38 AM
End Time   : 2013/07/16 1:39:38 AM
Notes      : 1. When the difference of Tx is less than the difference of Rx,
               the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
               ratio should be 100%;
             3. When calculate average loss and loss ratio, invalid or loc nodes
               will be excluded;
Latest single-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio
--------------------------------------------------------------------------------
1    all      0      000.0000%      0      000.0000%
2    all      0      000.0000%      0      000.0000%
3    all      0      000.0000%      0      000.0000%
4    all      0      000.0000%      0      000.0000%
5    all      0      000.0000%      0      000.0000%
6    all      0      000.0000%      0      000.0000%
7    all      0      000.0000%      0      000.0000%
8    all      0      000.0000%      0      000.0000%
9    all      0      000.0000%      0      000.0000%
--------------------------------------------------------------------------------
Maximum Local-loss  : 0        Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0        Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0        Average Local-loss Ratio  : 000.0000%
```

Maximum Remote-loss : 0 Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0 Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0 Average Remote-loss Ratio : 000.0000%

16.2.9 Configure Test

I. Topology

Please refer to CC Topology.

II. Configuration

Please refer to MD/MA/MEP configuration in CC.

Enable test function on Switch1 and Switch4.

Switch 1

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# ethernet cfm tst transmission enable domain cust vlan 30 mep 66 tx-mode continuous pattern-type random packet-size 64	Configure Test transmission function
Switch1 (config)# end	Exit configuration mode

Switch 4

Switch4# configure terminal	Enter global configuration mode
Switch4(config)# ethernet cfm tst reception enable domain cust vlan 30 mep 99	Configure Test reception function
Switch4 (config)# end	Exit configuration mode

III. Command validation

The following command is run for sending Test message from Switch1:

Switch1# ethernet cfm tst start rate 1000 time second 1

The following command is run for showing Test message on Switch1:

Switch1# show ethernet cfm tst
DOMAIN : cust
VLAN : 30
MEPID : 66
Transmission : Enabled
Reception : Disabled
Status : Non-Running
Start Time : 06:32:48

```
Predict End Time : 06:33:18
Actual End Time  : 06:33:18
Packet Type      : TST
Rate             : 1000 mbps
Packet Size      : 64 bytes
Tx Number        : 29
Tx Bytes         : 1856
Rx Number        : 0
Rx Bytes         : 0
```

The following command is run for showing Test message on Switch4:

```
Switch4#  show ethernet cfm tst
DOMAIN       : cust
VLAN         : 30
MEPID        : 99
Transmission  : Disabled
Reception     : Enabled
Status        : Non-Running
Start Time    : null
End Time      : null
Packet Type   : null
Rate          : null
Packet Size   : null
Tx Number     : 0
Tx Bytes      : 0
Rx Number     : 29
Rx Bytes      : 1856
```

16.3 CPU Traffic Configuration

16.3.1 Introduction

This chapter presents how to configure CPU traffic control and view CPU traffic.

CPU traffic control is a useful CPU protection mechanism realized by controlling the incoming data traffic of CPU.

CPU traffic control contains CPU protection measures at two levels:

The first is limiting reason traffic entering CPU. It is realized by configuring queue shaping corresponding to the reason in chip.

The second is limiting all data traffic entering CPU. It is realized by configuring shaping of CPU ports in chip.

Note: The “reason” mentioned here refers to the type of protocol messages, such as bgp, ospf, rip, and so much more.

The table below lists a series of reasons and corresponding descriptions:

Reason	Description
arp	Arp protocol message

Reason	Description
bpdu	Bpdu protocol message (including STP, RSTP, MSTP)
dhcp	dhcp protocol message
eapol	dot1x protocol message
erps	erps protocol message
fwd-to-cpu	Fowarding-to-cpu message
icmp-redirect	Icmmp redirect
igmp	IGMP or IGMP Snooping message
ip-option	IP message with optional field
ipda	ipda protocol message
ldp	ldp protocol message
macsa-mismatch	Learned message in the case of mismatching a port security entry
mcast-rpf-fail	Multicast message RPF check fail
mld	mld protocol message
mpls-ttl-fail	Ttl fail mpls message
ip-mtu-fail	Message to be segmented
ospf	ospf protocol message
pim	pim protocol message
port-security-discard	Learned message in the case of port security entry limit reached
rip	rip protocol message
sflow-egress	Egress sflow sampling message
sflow-ingress	Ingress sflow sampling message
slow-protocol	Bpdu protocol message (including EFM, LACP, SYNCE) Multicast message with ttl failure
smart-link	Smark link protocol message
ucast-ttl-fail	Unicast IP message with ttl failure
udld	udld protocol message
vlan-security-discard	Learned message in the case of learning mac limit in vlan reached
vrrp	vrrp protocol message

Reason	Description
bfd-learning	BFD learning message

16.3.2 Terms

PDU is short for protocol data unit.

16.3.3 Default Configuration

The default rate and priority configurations are as below:

Reason	rate(pps)	class	reason	rate(pps)	class
arp	640	1	mpls-ttl-fail	64	0
bpdu	64	3	ip-mtu-fail	64	0
dhcp	128	0	ospf	256	1
eapol	128	0	pim	128	1
erps	128	2	port-security-discard	128	0
fwd-to-cpu	64	0	rip	64	1
icmp-redirect	128	0	sflow-egress	128	0
igmp	128	2	sflow-ingress	128	0
ip-option	512	0	slow-protocol	128	1
ipda	1024	0	smart-link	128	2
ldp	512	1	ucast-ttl-fail	64	0
macsa-mismatch	128	0	udld	128	3
mcast-rpf-fail	128	1	vlan-security-discard	128	0
mld	128	2	vrrp	512	1
bfd-learning	128	1			

16.3.4 CPU Traffic Configuration

I. Total traffic limit configuration

Switch# configure terminal	Enter global configuration mode
Switch(config)# cpu-traffic-limit total rate 3000	Set total CPU traffic limit

II. Configure unit traffic limit

Switch# configure terminal	Enter global configuration mode
Switch(config)# cpu-traffic-limit reason rip rate 500	Set RIP PDU traffic limit

III. Configure priority class

Switch# configure terminal	Enter global configuration mode
Switch(config)# cpu-traffic-limit reason rip class 3	Change RIP PUD priority class

16.3.5 Command Validation

Use command “show cpu traffic-limit” to check configuration result, as below.

```
Switch# show cpu traffic-limit
reason                rate (pps)  class
dot1x-mac-bypass        64         2
bpdu                    64         3
slow-protocol           128        1
eapol                   128        0
erps                    128        2
smart-link              128        2
udld                    128        3
loopback-detection      64         3
arp                     256        1
dhcp                    128        0
rip                     500        3
ldp                     512        1
ospf                    256        1
pim                     128        1
vrrp                    512        1
ipda                    1024       0
icmp-redirect           128        0
mcast-rpf-fail          128        1
macsa-mismatch          128        0
port-security-discard   128        0
vlan-security-discard   128        0
mtu-dontfrag            64         0
mtu-frag                64         0
ip-mtu-fail             64         0
bfd-learning            128        1
ip-option               512        0
ucast-ttl-fail          64         0
mpls-ttl-fail           64         0
igmp                    128        2
sflow-ingress           128        0
sflow-egress            128        0
fwd-to-cpu              64         0
l2protocol-tunnel       1024       0
```

Total rate: 3000 (pps)

Use command “show cpu traffic-statistics receive all” to check traffic statistics, as below.

```
Switch# show cpu traffic-statistics receive all
statistics rate time is 5 second(s)
reason          count(packets)    rate(pps)
dot1x-mac-bypass      0              0
bpdu                  0              0
slow-protocol         0              0
eapol                 0              0
erps                  0              0
smart-link            0              0
udld                  0              0
loopback-detection    0              0
arp                   0              0
dhcp                  0              0
rip                   0              0
ldp                   0              0
ospf                  0              0
pim                   0              0
bgp                   0              0
vrrp                  0              0
rsvp                  0              0
ipda                  0              0
icmp-redirect         0              0
mcast-rpf-fail        0              0
macsa-mismatch        0              0
port-security-discard 0              0
vlan-security-discard 0              0
ip-mtu-fail           0              0
bfd-learning          0              0
ptp                   0              0
ip-option             0              0
tunnel-gre-keepalive  0              0
ucast-ttl-fail        0              0
mpls-ttl-fail         0              0
igmp                  0              0
sflow-ingress         0              0
sflow-egress          0              0
fwd-to-cpu            0              0
l2protocol-tunnel     0              0
mirror-to-cpu         0              0
mpls-tp-pwoam         0              0
other                 0              0
Total                 0              0
```

16.4 UDLD Configuration

16.4.1 Introduction

Unidirectional link detection (UDLD) is a lightweight protocol capable of detecting and disabling unidirectional link. Using UDLD can prevent the abnormal circumstance of some protocols such as spanning tree in the case of unidirectional link.

16.4.2 Topology

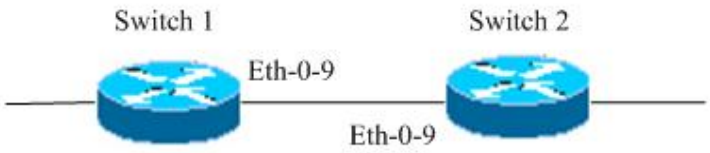


Figure 16-3 Typical UDLD Topology

16.4.3 Configuration

Switch 1

Enable UDLD protocol on eth-0-9 of Switch1.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# udld port	Enable UDLD protocol on the interface
Switch(config-if)# exit	Exit interface mode
Switch(config)# udld enable	Globally enable UDLD protocol
Switch(config)# udld message interval 10	Set UDLD message interval

Switch 2

Enable UDLD protocol on eth-0-9 of Switch2.

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-9	Enter interface mode
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# udld port	Enable UDLD protocol on the interface
Switch(config-if)# exit	Exit interface mode

Switch(config)# udld enable	Globally enable UDLD protocol
Switch(config)# udld message interval 10	Set UDLD message interval

16.4.4 Configuration Verification

Switch 1

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode        : normal
Operation state    : Bidirectional
Message interval  : 10
Message timeout   : 3
  Neighbor 1
  ---
  Device ID         : 4c7b.8510.ab00
  Port ID           : eth-0-9
  Device Name     : Switch
  Message interval: 10
  Message timeout : 3
  Link Status       : bidirectional
  Expiration time : 29
```

Switch 2

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode       : normal
Operation state   : Bidirectional
Message interval: 10
Message timeout : 3
  Neighbor 1
  ---
  Device ID         : 28bc.83db.8400
  Port ID           : eth-0-9
  Device Name     : Switch
  Message interval: 10
  Message timeout : 3
  Link Status       : bidirectional
  Expiration time   : 23
```

16.5 Smart-Link Configuration

16.5.1 Introduction

Smart link, also called backup link, is a solution to providing reliable efficient backup and handoff scheme for double-uplink, which is usually applied for double-uplink networking.

Comparing with spanning tree protocol (STP), smark link technology provides a faster convergence performance; comparing with ERPS, smart link provides a simpler configuration and usage mode.

The feature also has the function of link load balancing.

16.5.2 Topology

The below is a typical smart link configuration, with switches 1 and 2 as smart-link group and switches 3, 4 and 5 for smart link message receiving.

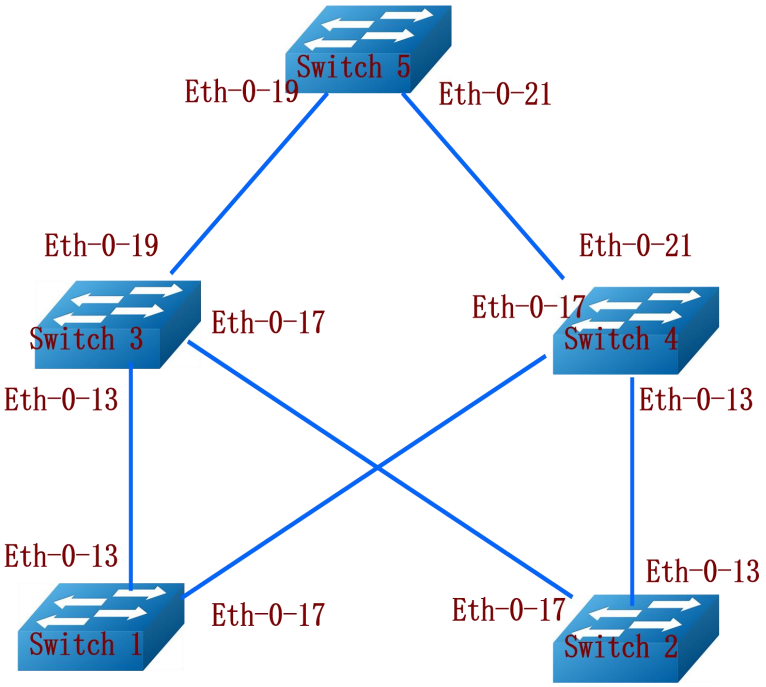


Figure 16-4 Smart-Link Typical Topology

16.5.3 Configuration

The example below shows configuration of smart link double-uplink protection, as shown in the topological graph 16-4.

Notes:

- The control vlan and protected vlan of smart link group must be created in the vlan database in advance.
- STP must be disabled on the ports of smart link group.
- The protected instance of smart link group must be created in MSTP module in advance.

Configure each switch with VLAN 1-300, MSTP instance1-3.

Switch 1 Configuration

Switch1# configure terminal	Enter configuration mode

Switch1 (config)# vlan database	Enter VLAN mode
Switch1(config- vlan)# vlan 2-20	Create VLAN 2-20
Switch1(config-vlan)# exit	Exit VLAN mode
Switch1(config)# spanning-tree mode mstp	Configure STP mode
Switch1(config)# spanning-tree mst configuration	Enter MSTP configuration mode
Switch1(config-mst)# instance 1 vlan 1	Configure association of MSTP instance 1 with VLAN 1
Switch1(config-mst)# instance 2 vlan 2	Configure association of MSTP instance 2 with VLAN 2
Switch1(config-mst)# instance 3 vlan 3	Configure association of MSTP instance 3 with VLAN 3
Switch1(config-mst)# exit	Exit MSTP configuration mode
Switch1(config)# interface eth-0-13	Enter interface 13
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# interface eth-0-17	Enter interface 17
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# smart-link group 1	Create group 1
Switch1(config-smlk-group)# interface eth-0-13 master	Assign the interface as master
Switch1(config-smlk-group)# interface eth-0-17 slave	Assign the interface as slave
Switch1(config-smlk-group)# protected mstp instance 1	Assign protected MSTP Instance

Switch1(config-smlk-group)# protected mstp instance 2	Assign protected MSTP Instance
Switch1(config-smlk-group)# protected mstp instance 3	Assign protected MSTP Instance
Switch1(config-smlk-group)# load-balance instance 3	Enable load-balance Instance
Switch1(config-smlk-group)# restore time 40	Set automatic switching waiting time within the range of 30s-1200s
Switch1(config-smlk-group)# restore enable	Enable automatic switching
Switch1(config-smlk-group)# flush send control-vlan 10 password simple test	Set control VLAN and specify the password of Smart-link receiving end
Switch1(config-smlk-group)# group enable	Enable smart link group
Switch1(config-smlk-group)# end	Exit group mode

Switch2 configuration is same with that of Switch1.

Switch 3 Configuration

Switch3# configure terminal	Enter configuration mode
Switch3(config)# interface eth-0-13	Enter interface 13
Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# no shutdown	Open the interface
Switch3(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	Set control VLAN and specify the password of Smart-link receiving end
Switch3(config-if)# exit	Exit interface mode
Switch3(config)# interface eth-0-17	Enter interface 17
Switch3(config-if)# no shutdown	Open the interface
Switch3(config-if)# switchport mode trunk	Configure the port as trunk
Switch3(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	Set control VLAN and specify the password of Smart-link receiving end
Switch3(config-if)# exit	Exit interface mode

NOTE

Switch 4 configuration is same with that of Switch 3.

Switch 5 Configuration

Switch5# configure terminal	Enter configuration mode
Switch5(config)# interface eth-0-19	Enter interface 19
Switch5(config-if)# switchport mode trunk	Configure the port as trunk
Switch5(config-if)# no shutdown	Open the interface
Switch5(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch5(config-if)# smart-link flush receive control-vlan 10 password simple test	Set control VLAN and specify the password of Smart-link receiving end
Switch5(config-if)# exit	Exit interface mode
Switch5(config)# interface eth-0-21	Enter interface 21
Switch5(config-if)# switchport mode trunk	Configure the port as trunk
Switch5(config-if)# no shutdown	Open the interface
Switch5(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
smart-link flush receive control-vlan 10 password simple test	Set control VLAN and specify the password of Smart-link receiving end
Switch5(config-if)# exit	Exit interface mode
Switch5(config)# no smart-link relay enable	Disable relay function

16.5.4 Command Validation

Switch 1

Switch1# show smart-link group 1

```
Smart-link group 1 information:
The smart-link group was enabled.
============================================================
Auto-restore:
  state      time          count    Last-time
  enabled    40              0      N/A
============================================================
Protected instance: 1  2  3
Load balance instance: 3
```

```
Flush sender , Control-vlan ID: 10    Password:test
============================================================
INTERFACE:
Role   Member    DownCount Last-Down-Time  FlushCount Last-Flush-Time
MASTER eth-0-13   0       N/A                0     N/A
SLAVE    eth-0-17   0       N/A                0     N/A
============================================================
Instance states in the member interfaces:
 A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
Map-instance-ID   MASTER(eth-0-13)    SLAVE(eth-0-17)
    1             A                   B
    2             A                   B
    3             B                   A
```

Switch 2

Switch2# show smart-link group 1

```
Smart-link group 1 information:
The smart-link group was enabled.
============================================================
Auto-restore:
 state      time          count    Last-time
 enabled    40              0      N/A
============================================================
Protected instance: 1  2  3
Load balance instance: 3
Flush sender , Control-vlan ID: 10    Password:test
============================================================
INTERFACE:
Role   Member    DownCount Last-Down-Time  FlushCount Last-Flush-Time
MASTER eth-0-13   0       N/A                0     N/A
SLAVE    eth-0-17   0       N/A                0     N/A
============================================================
Instance states in the member interfaces:
 A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
Map-instance-ID   MASTER(eth-0-13)    SLAVE(eth-0-17)
    1             A                   B
    2             A                   B
    3             B                   A
```

Switch 3

Switch3# show smart-link

```
Relay smart-link flush packet is enabled
Smart-link flush receiver interface:
   eth-0-13   control-vlan:10   password:test
   eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch 4

Switch4# show smart-link

```
Relay smart-link flush packet is enabled
Smart-link flush receiver interface:
  eth-0-13   control-vlan:10   password:test
  eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch 5

Switch5# show smart-link

```
Relay smart-link flush packet is disabled
Smart-link flush receiver interface:
  eth-0-21   control-vlan:10   password: test
  eth-0-19   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

16.6 Multi-Link Configuration

16.6.1 Introduction

Multi-link, also called multi-backup link, is a solution to providing reliable efficient backup and handoff scheme for multi-uplink. This function is similar to smart link. The backup links have been increased to multiple links, and up to 4 members are supported.

The feature also has the function of link load balancing.

16.6.2 Topology

The below is a multi-link typical configuration, with switch 1 as multi-link group and switches 2, 3, 4 and 5 for multi-link message receiving.

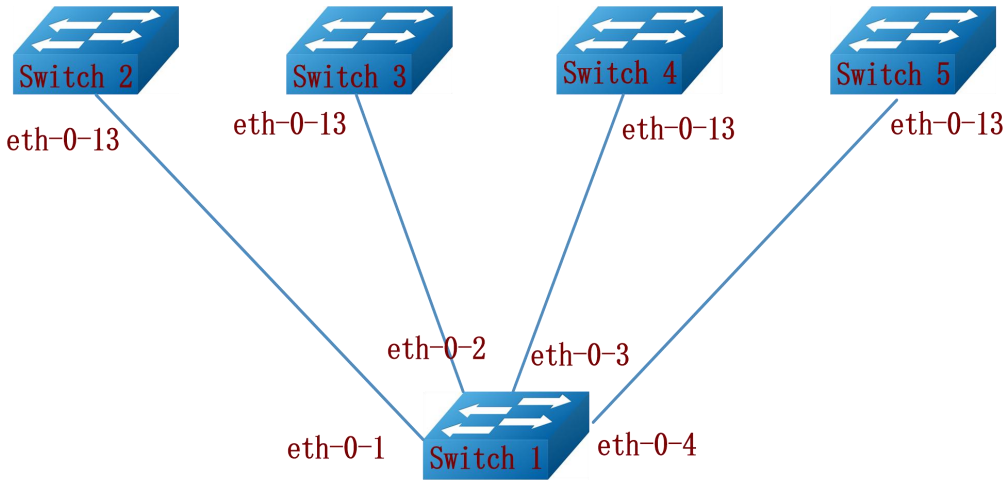


Figure 16-5 Multi-Link Typical Topology

16.6.3 Configuration

The example below shows configuration of multi-uplink protection of multi-link, as shown in the topological graph 16-4.

Notes:

- The control vlan and protected vlan of Multi-link group must be created in the vlan database in advance.
- STP must be disabled on the ports of Multi-link group.
- The protected instance of Multi-link group must be created in MSTP module in advance.

Configure each switch with VLAN 2-10, MSTP instance1-4.

Switch 1 Configuration

Switch1# configure terminal	Enter configuration mode
Switch1 (config)# vlan database	Enter VLAN mode
Switch1(config- vlan)# vlan 2-10	Create VLAN 2-10
Switch1(config-vlan)# exit	Exit VLAN mode
Switch1(config)# spanning-tree mode mstp	Configure STP mode
Switch1(config)# spanning-tree mst configuration	Enter MSTP configuration mode

Switch1(config-mst)# instance 1 vlan 1	Configure association of MSTP instance 1 with VLAN 1
Switch1(config-mst)# instance 2 vlan 2	Configure association of MSTP instance 2 with VLAN 2
Switch1(config-mst)# instance 3 vlan 3	Configure association of MSTP instance 3 with VLAN 3
Switch1(config-mst)# instance 4 vlan 4-10	Configure association of MSTP instance 4 with VLAN 4
Switch1(config-mst)# exit	Exit MSTP configuration mode
Switch1(config)# interface range eth-0-1 - 4	Enter interface 1-4
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# multi-link group 1	Create group 1
Switch1(config-multilk-group)# interface eth-0-1 priority 1	Assign interface 1 priority as 1
Switch1(config-multilk-group)# interface eth-0-2 priority 2	Assign interface 2 priority as 2
Switch1(config-multilk-group)# interface eth-0-3 priority 3	Assign interface 3 priority as 3
Switch1(config-multilk-group)# interface eth-0-4 priority 4	Assign interface 4 priority as 4
Switch1(config-multilk-group)# protected mstp instance 1	Assign protected MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 2	Assign protected MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 3	Assign protected MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 4	Assign protected MSTP Instance
Switch1(config-multilk-group)# load-balance instance 2 priority 2	Enable load-balance Instance
Switch1(config-multilk-group)# load-balance instance 3 priority 3	Enable load-balance Instance

Switch1(config-multilk-group)# load-balance instance 4 priority 4	Enable load-balance Instance
Switch1(config-multilk-group)# restore time 40	Set automatic switching waiting time within the range of 30s-1200s
Switch1(config-multilk-group)# restore enable	Enable automatic switching
Switch1(config-multilk-group)# flush send control-vlan 10 password simple test	Set control VLAN and specify the password of Multi-link receiving end
Switch1(config-multilk-group)# group enable	Enable Multi-link group
Switch1(config-multilk-group)# end	Exit group mode

Switch 2 Configuration

Switch2# configure terminal	Enter configuration mode
Switch2(config)# interface eth-0-13	Enter interface 13
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch2(config-if)# multi-link flush receive control-vlan 10 password simple test	Set control VLAN and specify the password of Multi-link receiving end
Switch2(config-if)# exit	Exit interface mode

Switch 3 -5 configuration is same with that of Switch 2.

16.6.4 Command Validation

Switch 1

Switch1# show multi-link group 1

```
Multi-link group 1 information:
 The multi-link group was enabled.
==========================================================
 Auto-restore:
```

```
  state       time          count    Last-time
  enabled     40              0      N/A
==========================================================
Protected instance: 1  2  3  4
Load balance instance: 2(to P2)  3(to P3)  4(to P4)
Flush sender , Control-vlan ID: 10    Password:test
==========================================================
INTERFACE:
Role   Member    DownCount Last-Down-Time      FlushCount Last-Flush-Time
PRI1   eth-0-1   0         N/A                 1          2016/09/05,07:13:24
PRI2   eth-0-2   0         N/A                 1          2016/09/05,07:13:24
PRI3   eth-0-3   0         N/A                 1          2016/09/05,07:13:24
PRI4   eth-0-4   0         N/A                 1          2016/09/05,07:13:24
==========================================================
Instance states in the member interfaces:
  A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
Map-instance-ID  P1(eth-0-1 )  P2(eth-0-2 )  P3(eth-0-3 )  P4(eth-0-4 )
1                A             B             B             B
2                B             A             B             B
3                B             B             A             B
4                B             B             B             A
```

Switch 2

Switch2# show multi-link

```
Relay multi-link flush packet is enabled
Multi-link flush receiver interface:
   eth-0-13   control-vlan:10   password:test
Multi-link received flush packet number:0
Multi-link processed flush packet number:0
Multi-link tcn is disabled
Multi-link tcn query count    :2
Multi-link tcn query interval :10
Multi-link Group Number is 0.
```

16.7 Multi-Link Enhance Configuration

16.7.1 Introduction

Multi-link, also called multi-backup link, is a solution to providing reliable efficient backup and handoff scheme for multi-uplink. This function is similar to smart link. The backup links have been increased to multiple links, and up to 4 members are supported.

If two groups of multi-links distributed on different switches act as link backup for each other, the mutual link backup might fail due to the protected instance of multi-link member of one side being blocked.

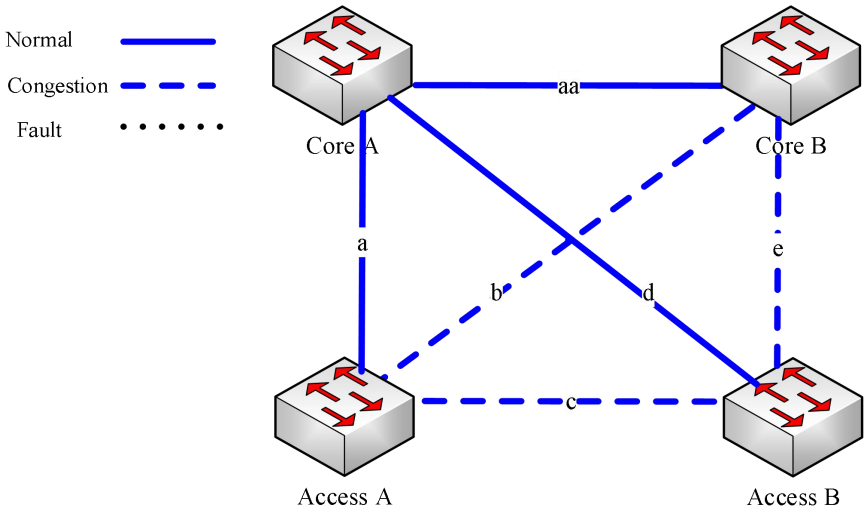
Such as the following user scenarios:

Core switch A, core switch B, access switch A, and access switch B form a full mesh topology.

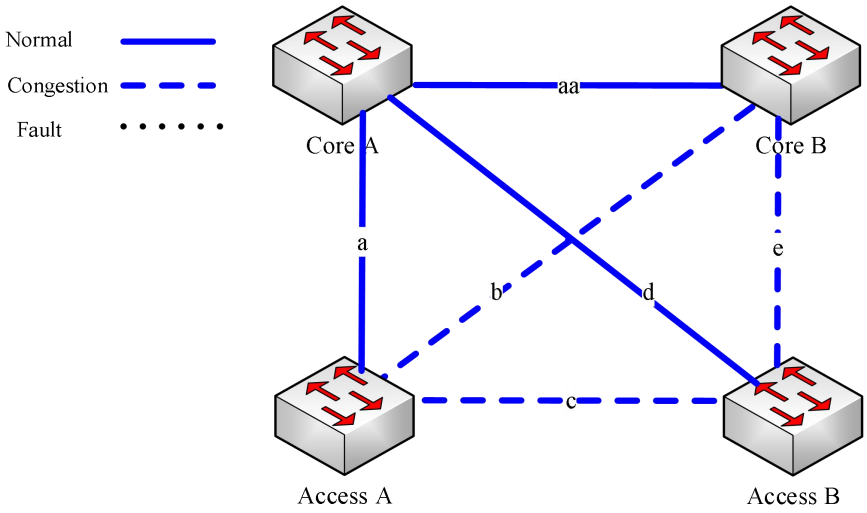
Access switch A is configured with multi-link protocol, and the priority class of links a, b and c is 1, 2 and 3 respectively;

Access switch B is configured with multi-link protocol, and the priority class of links d and e is 1 and 2 respectively;

Under normal circumstances, links b, c and e are in block state, and links a and d are in active state, as shown in the figure below:



When links d and e of access switch B all are disconnected, only link c remains connected to access switch A, as shown in the figure below:



In this case, link aof access switch A is in active state, the port of switch A corresponding to link c is in block state, and access switch B is in an island state.

16.7.2 Topology

The below is a multi-link typical configuration, where switches 1 and 2 both are configured with multi-link group. Switch 1 multi-link group is allocated with three members, and the member of the lowest priority is a multi-link enhance receiving port. Switch 2 multi-link group is allocated with two members as well as a multi-link enhance sending port.

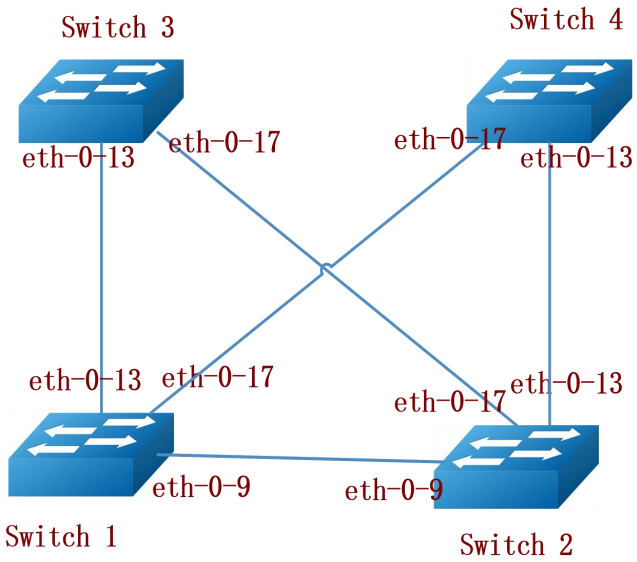


Figure 6-6 Multilink-enhance Typical Topology

16.7.3 Configuration

The example below shows configuration of multi-uplink protection of multi-link, as shown in the topological graph 16-4.

Notes:

- The control vlan and protected vlan of Multi-link group must be created in the vlan database in advance.
- STP must be disabled on the ports of Multi-link group.
- The protected instance of Multi-link group must be created in MSTP module in advance.
- For multi-link group, the control vlan and password of flush send must be configured first, followed by multilink enhance

Configure each switch with VLAN 10, 20, 30 and 40, as well as MSTP instance1 and 2.

Switch 1 Configuration

Switch1# configure terminal	Enter configuration mode
Switch1 (config)# vlan database	Enter VLAN mode
Switch1 (config-vlan)# vlan 10	Create VLAN 10
Switch1 (config-vlan)# vlan 20	Create VLAN 20
Switch1 (config-vlan)# vlan 30	Create VLAN 30
Switch1 (config-vlan)# vlan 40	Create VLAN 40

Switch1(config-vlan)# exit	Exit VLAN mode
Switch1(config)# spanning-tree mode mstp	Configure STP mode
Switch1(config)# spanning-tree mst configuration	Enter MSTP configuration mode
Switch1(config-mst)# instance 1 vlan 10	Configure association of MSTP instance 1 with VLAN 10
Switch1(config-mst)# instance 1 vlan 30	Configure association of MSTP instance 1 with VLAN 30
Switch1(config-mst)# instance 2 vlan 20	Configure association of MSTP instance 2 with VLAN 20
Switch1(config-mst)# instance 2 vlan 40	Configure association of MSTP instance 2 with VLAN 40
Switch1(config-mst)# exit	Exit MSTP configuration mode
Switch1(config)# interface range eth-0-9	Enter interface 9
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# interface range eth-0-13	Enter interface 13
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# interface range eth-0-17	Enter interface 17
Switch1(config-if)# switchport mode trunk	Configure the port as trunk
Switch1(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch1(config-if)# spanning-tree port disable	Disable STP on the port
Switch1(config-if)# no shutdown	Open the interface

Switch1(config-if)# exit	Exit interface mode
Switch1(config)# multi-link group 1	Create group 1
Switch1(config-multilk-group)# interface eth-0-13 priority 1	Assign interface 13 priority as 1
Switch1(config-multilk-group)# interface eth-0-17 priority 2	Assign interface 17 priority as 2
Switch1(config-multilk-group)# interface eth-0-9 priority 3	Assign interface 9 priority as 3
Switch1(config-multilk-group)# protected mstp instance 1	Assign protected MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 2	Assign protected MSTP Instance
Switch1(config-multilk-group)# flush send control-vlan 30 password simple a	Set control VLAN and specify the password of Multi-link sending end
Switch1(config-multilk-group)# multilink-enhance receive control-vlan 10 password b interface eth-0-9	Enable interface eth-0-9 to receive multilink-enhance message
Switch1(config-multilk-group)# group enable	Enable Multi-link group
Switch1(config-multilk-group)# end	Exit group mode

Switch 2 Configuration

Switch2# configure terminal	Enter configuration mode
Switch2 (config)# vlan database	Enter VLAN mode
Switch2 (config-vlan)# vlan 10	Create VLAN 10
Switch2 (config-vlan)# vlan 20	Create VLAN 20
Switch2(config-vlan)# exit	Exit VLAN mode
Switch2(config)# spanning-tree mode mstp	Configure STP mode
Switch2(config)# spanning-tree mst configuration	Enter MSTP configuration mode
Switch2(config-mst)# instance 1 vlan 10	Configure association of MSTP instance 1 with VLAN 10
Switch2(config-mst)# instance 2 vlan 20	Configure association of MSTP instance 2 with VLAN 20
Switch2(config-mst)# exit	Exit MSTP configuration mode

Switch2(config)# interface eth-0-13	Enter interface 13
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-17	Enter interface 13
Switch2(config-if)# switchport mode trunk	Configure the port as trunk
Switch2(config-if)# switchport trunk allowed vlan all	Set the port to allow all VLANs
Switch2(config-if)# no shutdown	Open the interface
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# multi-link group 1	Create group 1
Switch2(config-multilk-group)# interface eth-0-13 priority 1	Assign interface 13 priority as 1
Switch2(config-multilk-group)# interface eth-0-17 priority 2	Assign interface 17 priority as 2
Switch2(config-multilk-group)# protected mstp instance 1	Assign protected MSTP Instance
Switch2(config-multilk-group)# protected mstp instance 2	Assign protected MSTP Instance
Switch2(config-multilk-group)# flush send control-vlan 10 password simple b	Set control VLAN and specify the password of Multi-link sending end
Switch2(config-multilk-group)# multilink-enhance interface eth-0-9	Set an interface for sending multilink enhance message
Switch2(config-multilk-group)# group enable	Enable Multi-link group
Switch2(config-multilk-group)# exit	Exit group mode
Switch2(config)# interface eth-0-9	Enter interface configuration mode
Switch2(config-if)# multi-link flush receive control-vlan 30 password simple a	Enable the interface to receive flush message with control vlan id and password consistent with flush send configured on switch1
Switch2(config-if)# end	Exit interface mode

NOTE

Switch3-4 configure has to accept the rhythm of flush message only.

16.7.4 Command Validation

Switch 1

Switch1# show multi-link group 1

```
Multi-link group 1 information:
The multi-link group was enabled.
============================================================
Auto-restore:
  state       time          count     Last-time
  disabled    60            0         N/A
============================================================
Protected instance: 1  2
Load balance instance:
Flush sender , Control-vlan ID: 30    Password: a
============================================================
INTERFACE:
Role   Member     DownCount Last-Down-Time      FlushCount Last-Flush-Time
PRI1   eth-0-13    0          N/A                5          2017/05/15,07:50:11
PRI2   eth-0-17    0          N/A                0          N/A
PRI3   eth-0-9     1          2017/05/15,07:48:46 5         2017/05/15,07:50:11
PRI4   N/A         0          N/A                0          N/A
============================================================
Instance states in the member interfaces:
  A-ACTIVE ,    B-BLOCK ,  A(E)-ENHANCE_ACTIVE    D-The interface is link-down
Map-instance-ID  P1(eth-0-13)    P2(eth-0-17)    P3(eth-0-9)     P4(N/A)
1                A               B               B               D
2                A               B               B               D
Switch1# show multi-link
Relay multi-link flush packet is enabled
Multi-link enhance receiver interface:
   eth-0-9    control-vlan:10   password:b
Multi-link received flush packet number : 0
Multi-link processed flush packet number: 0
Multi-link received enhance packet number : 4
Multi-link processed enhance packet number: 4
Multi-link tcn is disabled
Multi-link tcn query count    : 2
Multi-link tcn query interval : 10
Multi-link Group Number is 1.
 Group-ID    State       Pri-1     Pri-2     Pri-3     Pri-4
 1           enabled     eth-0-13  eth-0-17  eth-0-9   N/A
```

Switch 2

Switch2# show multi-link group1

```
Multi-link group 1 information:
The multi-link group was enabled.
```

```
==========================================================
Auto-restore:
  state       time          count     Last-time
  disabled    60            0         N/A
==========================================================
Protected instance: 1  2
Load balance instance:
Flush sender , Control-vlan ID: 10    Password: b
Multilk enhance interface: eth-0-9, Control-vlan ID: 10  Password: b
==========================================================
INTERFACE:
Role   Member    DownCount Last-Down-Time      FlushCount Last-Flush-Time
PRI1   eth-0-13  1         2017/05/15,07:49:15 0          N/A
PRI2   eth-0-17  2         2017/05/15,07:50:03 3          2017/05/15,07:50:11
PRI3   N/A       0         N/A                 0          N/A
PRI4   N/A       0         N/A                 0          N/A
==========================================================
ENHANCE INTERFACE:
 Role   Member    DownCount Last-Down-Time      EnhanceCount Last-SendEnhance-Ti
me
M-En   eth-0-9   0         N/A                 0          N/A


==========================================================
Instance states in the member interfaces:
  A-ACTIVE ,    B-BLOCK ,  A(E)-ENHANCE_ACTIVE    D-The interface is link-down
Map-instance-ID  P1(eth-0-13)    P2(eth-0-17)    P3(N/A)         P4(N/A)
1                A               B               D               D
2                A               B               D               D
Switch2# show multi-link
Relay multi-link flush packet is enabled
Multi-link received flush packet number : 0
Multi-link processed flush packet number: 0
Multi-link received enhance packet number : 0
Multi-link processed enhance packet number: 0
Multi-link tcn is disabled
Multi-link tcn query count    : 2
Multi-link tcn query interval : 10
Multi-link Group Number is 1.
 Group-ID    State       Pri-1      Pri-2      Pri-3      Pri-4
 1           enabled     eth-0-13   eth-0-17   N/A        N/A
```

16.8 Monitor-Link Configuration

16.8.1 Introduction

Monitor link is a port linkage scheme introduced to supplement smart link, which is for extending the scope of link backup of smart link. It realizes synchronization setting of down link by monitoring up linking, so that up link failure can be conveyed to downstream equipment to trigger the main standby link switch of smart link and prevent flow loss due to long-time up link failure.

16.8.2 Topology

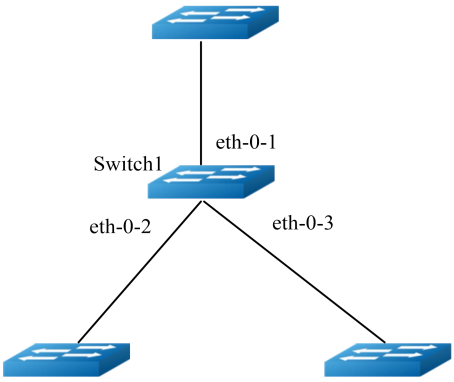


Figure 16-7 Configure monitor link

16.8.3 Configuration

Switch1# configure terminal	Enter configuration mode
Switch1(config)# interface range eth-0-1 - 3	Enter interface mode
Switch1(config-if-range)# no shutdown	Open the interface
Switch1(config-if-range)# exit	Exit interface mode
Switch1(config)# multi-link group 1	Create monitor link group 1
Switch1(config-mtlk-group)# monitor-link uplink interface eth-0-1	Set eth-0-1 as uplink interface
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-2	Set eth-0-2 as downlink interface
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-3	Set eth-0-3 as downlink interface
Switch1(config-mtlk-group)# end	Exit monitor link mode

16.8.4 Validation

Switch1# show monitor-link group

```
Group Id: 1
Monitor link status: UP
Role    Member   Last-up-time      Last-down-time       upcount  downcount
UpLk 1  eth-0-1  2011/07/15,02:07:31  2011/07/15,02:07:31  2       1
DwLk 1  eth-0-2  2011/07/15,02:07:34  2011/07/15,02:07:31  1       1
DwLk 2  eth-0-3  N/A                  N/A                  0       0
```

16.9 VRRP Configuration

16.9.1 Introduction

Generally, all hosts in a subnet are set with a same default route to the gateway. All messages with destination addresses not in the current network segment sent from the hosts will be sent to the gateway via the default route to realize communication between the hosts with the external network. In the case of gateway failure, the communication between all hosts with the gateway as default gateway in this network segment and the external network will be interrupted.

Default route facilitates users configuring operation, but demands extremely high stability of default gateway device. The common method of enhancing system reliability is to increase exit gateway. Following the increase of exit gateway, how to route among several outlets becomes another question.

Virtual router redundancy protocol (VRRP) can solve the problem above. In an LAN (such as Ethernet) capable of multicasting or broadcasting, VRRP can be leveraged to provide highly reliable default link even in the case of failure of some device, without modifying user's configuration information.

VRRP makes a set of routers (including a master router and several backup routers) into a backup team equal to a virtual router functionally.

VRRP backup team has the following features:

The hosts in the LAN must know the IP address of the virtual router only, and set it as the next hop address of the default route.

The hosts in the network communicate with the external network via the virtual router.

The routers of the backup team serve as gateway respectively in accordance with certain election mechanism. In the event that the router serving as gateway breaks down, other routers of the backup team will replace it to serve as gateway.

16.9.2 References

VRRP references are as below:

RFC 3768 (VRRP): Knight, S., et.al "Virtual Router Redundancy Protocol (VRRP)

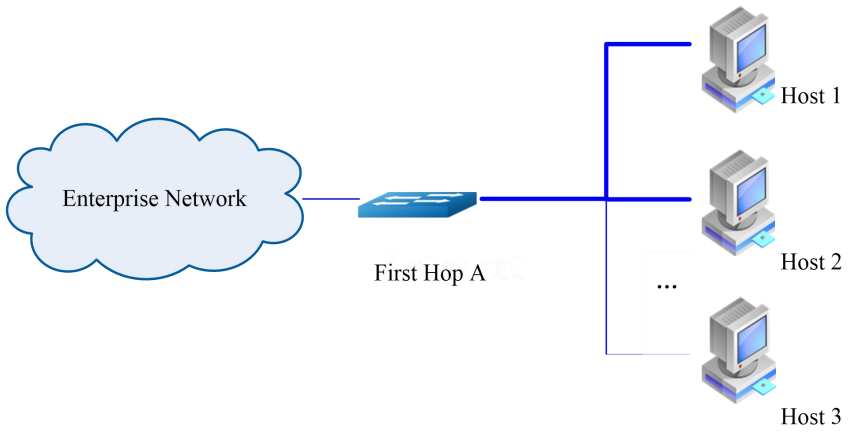
16.9.3 Terms

- **Backup router:** Backup router of VRRP. The backup router is enabled if the master router fails in forwarding.
- **Critical IP:** IP address for VRRP router sending/receiving a specific session information.
- **IP Address Owner:** VRRP router takes the IP address of the virtual router as a real interface address. When the device works normally, it will respond to messages with a virtual address as the destination address, such as ping, TCP connection, etc.
- **Master Router:** A router with a virtual IP address. It becomes the default gateway of the hosts to forward data flow.
- **Virtual IP:** IP address of virtual router. One virtual router can have one IP address, which is configured by user.

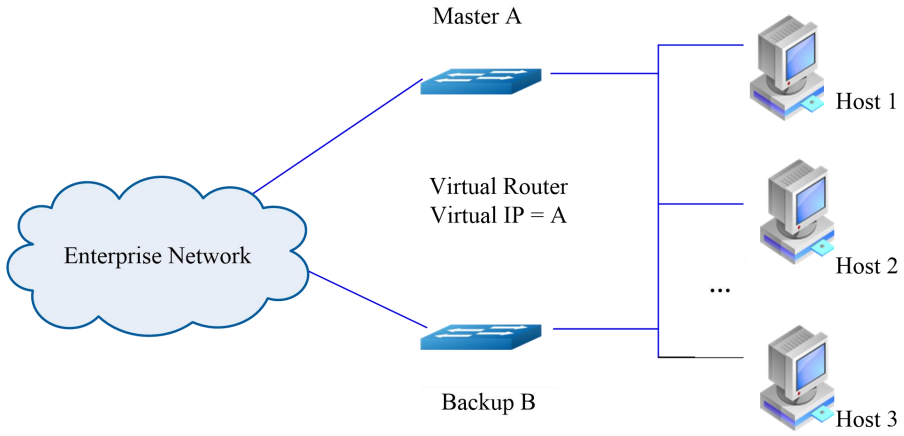
- **Virtual Router:** An abstract device under VRRP management, also called VRRP backup team, is taken as the default gateway of hosts of a shared LAN. It contains a virtual router identifier and a virtual IP address.
- **VRRP Router:** A device for running VRRP that may belong to one or more virtual routers.

16.9.4 VRRP Process

In general, terminal host connects to enterprise network via routers in the same LAN as its first next hop. It is common for terminal host to be statically configured with the default gateway. This can minimize the cost of configuration and processing. The major problem of this configuration is that if routers of the first next hop go wrong, a single point of failure will be caused.



VRRP attempts to introduce a concept of virtual router to solve this problem, which consists of two or more VRRP routers in one subnet. Meanwhile, it also introduces a concept of virtual IP address that is taken by terminal hosts as their default gateway address. Only the master router is responsible for forwarding data packets. If the master router breaks down, one of other routers (backup) replaces the master router to forward data packets.



The abovementioned configurations might not be useful, because the cost will be doubled, and a router will be left unused in most time. We can avoid this problem by building two virtual routers for load sharing.

16.9.5 Configure VRRP (One Virtual Router)

Active-standby mode means that the service is assumed by the master router only. Only if the master router goes wrong, a router will be elected from other backup routers to take over. Active-standby mode needs one backup team only, the routers of this backup team have different priorities, and the one of the highest priority will become the master router.

In the example below, all terminal hosts take virtual router 1 as their default gateway. VRRP protocol is running on both Routers R1 and R2. RI is configured as the master router of virtual router 1 (VRID = 1), and R2 as a backup router of virtual router 1. If R1 goes wrong, R2 will take over forwarding and render uninterrupted services to the hosts. This configuration involves one virtual router only, and R2 is left unused.

I. Topology

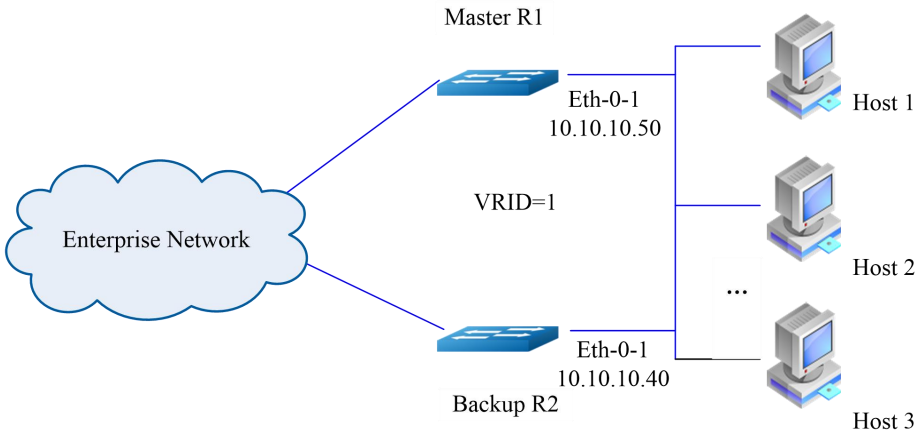


Figure 16-8 Single VRRP Router

II. Configuration

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter port mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.50/24	Set IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router vrrp 1	Create virtual router group 1
Switch(config-router)# virtual-ip 10.10.10.50	Set virtual IP address.
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval	Configure advertisement interval

5	
Switch (config-router)# bfd 10.10.10.40	Configure BFD session
Switch(config-router)# enable	Enable VRRP group 1

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter port mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.40/24	Set IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router vrrp 1	Create VRRP virtual router group 1
Switch(config-router)# virtual-ip 10.10.10.50	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# priority 200	Configure VRRP priority
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval
Switch (config-router)# bfd 10.10.10.50	Configure BFD session
Switch(config-router)# enable	Enable VRRP group 1

16.9.6 Configure VRRP (Two Virtual Routers)

Multiple backup teams can be built on one interface of router so that the router can serve as the master router in one backup team and as a backup router in other teams.

Load sharing refers to that multiple routers share the load simultaneously. Thus, load sharing requires two or more backup teams that consist of one master router and several backup routers respectively. The master router of each backup team can be different from one another.

The example below shows how to realize load sharing with two virtual routers. R1 and R2 forward different data packets respectively, and they back up for each other to ensure traffic load balancing.

I. Topology

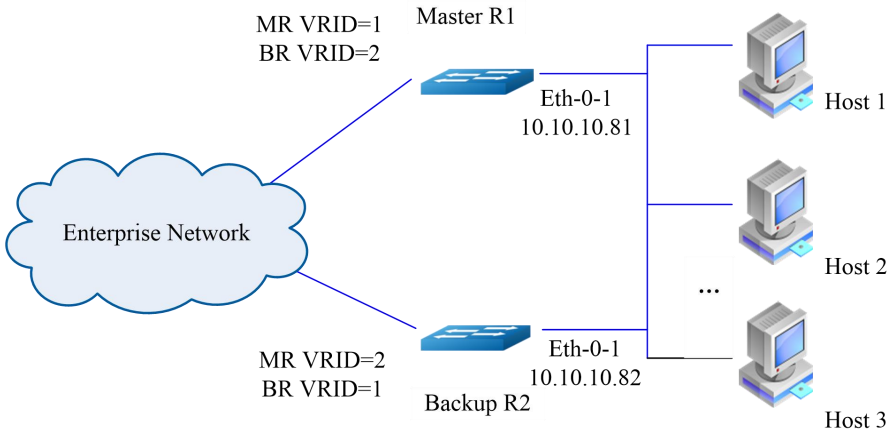


Figure 16-9 Two Virtual Router

II. Configuration

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as layer3 interface
Switch(config-if)# ip address 10.10.10.81/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router vrrp 1	Create VRRP virtual router group 1
Switch(config-router)# virtual-ip 10.10.10.81	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval as 5 seconds
Switch(config-router)# enable	Enable VRRP group 1
Switch(config-router)# exit	Exit routing mode
Switch(config)# router vrrp 2	Create VRRP virtual router group 2
Switch(config-router)# virtual-ip 10.10.10.82	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# priority 200	Configure VRRP priority
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)#	Configure advertisement interval as 5

advertisement-interval 5	seconds
Switch (config-router)# bfd 10.10.10.82	Configure BFD session
Switch(config-router)# enable	Enable VRRP group 2

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set layer3 interface
Switch(config-if)# ip address 10.10.10.82/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router vrrp 1	Create VRRP virtual router group 1
Switch(config-router)# virtual-ip 10.10.10.81	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# priority 200	Configure VRRP priority
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval as 5 seconds
Switch(config-router)# enable	Enable VRRP group 1
Switch(config-router)# exit	Exit routing mode
Switch(config)# router vrrp 2	Create VRRP virtual router group 2
Switch(config-router)# virtual-ip 10.10.10.82	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval as 5 seconds
Switch (config-router)# bfd 10.10.10.81	Configure BFD session
Switch(config-router)# enable	Enable VRRP group 2

III.Command validation

```
Switch# show vrrp 1
VRID <1>
 State            : Initialize(Interface down)
 Virtual IP       : 10.10.10.81(IP owner)
```

```
 Interface            : eth-0-1
 VMAC                 : 0000.5e00.0101
 VRF                  : Default
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : Unset        Run pri   : 255
 Master router ip     : Unknown
 Master priority      : Unknown
 Master advt timer    : Unknown
 Master down timer    : Unknown
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
Switch# show vrrp 2
VRID <2>
 State                : Initialize(Interface down)
 Virtual IP           : 10.10.10.82(Not IP owner)
 Interface            : eth-0-1
 VMAC                 : 0000.5e00.0102
 VRF                  : Default
 Advt timer           : 5 second(s)
 Preempt mode         : TRUE
 Conf pri             : 200          Run pri   : 200
 Master router ip     : Unknown
 Master priority      : Unknown
 Master advt timer    : Unknown
 Master down timer    : Unknown
 Preempt delay        : 0 second(s)
 Learn master mode    : FALSE
```

16.9.7 Configure VRRP Circuit Failover

The VRRP link failure detection function is needed because VRRPv2 is incapable of tracing the uplink status of gateway. The monitor over uplink helps effectively drive virtual router switching to avoid “black hold router”. In the case of uplink interface failure of master router, the former master router will switch to a backup router, and the former backup router will replace the master router.

To realize the VRRP link failure detection function, we must configure a priority-delta value for the monitored interface, and the value will be attached to the master router to realize the switch of VRRP router from master to backup.

As shown in the example below, the two routers R1 and R2 are configured with different priorities, and the priority-delta value must be larger than the difference between R1 priority and R2 priority. R1 priority is set as 100, and R2 priority as 90. R1 becomes the master router for a higher priority. The priority-delta value is set as 20. R1 priority will become 80 (100-20) if the uplink eth2 of RI goes wrong. In such case, R2 priority is higher than R1 priority, so R2 becomes the master router. When R1 is stored, it becomes the master router again because its priority is 100.

I. Topology

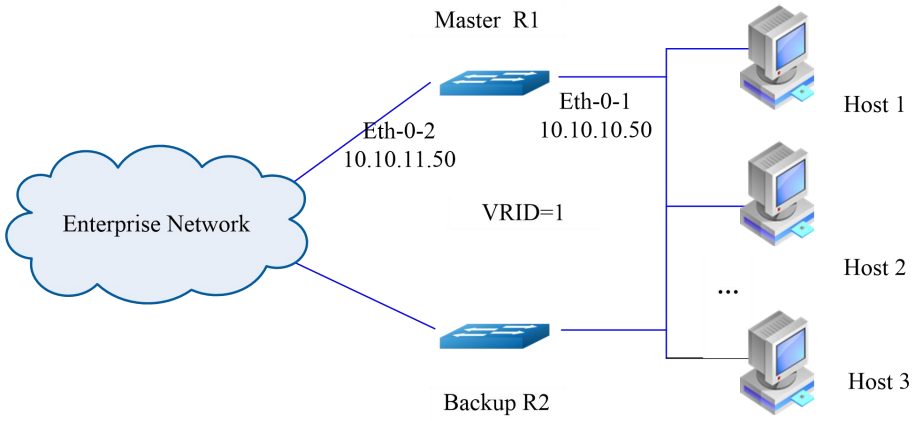


Figure 16-10 VRRP Example

II. Configuration

R1

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set layer3 interface
Switch(config-if)# ip address 10.10.10.50/24	Configure IP address
Switch(config-if)# exit	Exit interface address
Switch(config)# interface eth-0-2	Enter interface mode
Switch(config-if)# no switchport	Set layer3 interface
Switch(config-if)# ip address 10.10.11.50/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# track 10 interface eth-0-2 linkstate	Set interface linkstate as track condition
Switch(config)# router vrrp 1	Create VRRP group 1
Switch(config-router)# virtual-ip 10.10.10.1	Specify virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval as 5 seconds
Switch(config-router)# priority 100	Configure VRRP priority as 100
Switch(config-router)# track 10 decrement 20	Track 10 and priority-delta value 20

Switch(config-router)# enable	Enable VRRP group 1

R2

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set layer3 interface
Switch(config-if)# ip address 10.10.10.40/24	Configure IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# router vrrp 1	Create VRRP group 1
Switch(config-router)# virtual-ip 10.10.10.1	Set virtual IP address
Switch(config-router)# interface eth-0-1	Configure application port of VRRP group
Switch(config-router)# preempt-mode true	Set preempt mode
Switch(config-router)# advertisement-interval 5	Configure advertisement interval as 5 seconds
Switch(config-router)# priority 90	Configure priority 90
Switch(config-router)# enable	EnableVRRP1

16.9.8 Limit

VRRP doesn't support MD5 authentication.

16.10 Track Configuration

16.10.1 Configure IP SLA

I. Introduction

IP service level agreement (SLA) is a measuring and diagnostic tool for implementing network performance by means of “dynamic monitoring”. “Dynamic monitoring” refers to measuring network connectivity and network performance by means of ping on switches. Every IP SLA operation will maintain a returned value generated from its operation. The returned value will be interrupted by tracking process. The returned value might be “OK” or other codes if exceeding the threshold. Different operations lead to different returned values. In the system, only the returned values applicable to all operation types are adopted. In IPSLA, we can check status or routability via ICMP echo.

II. Topology

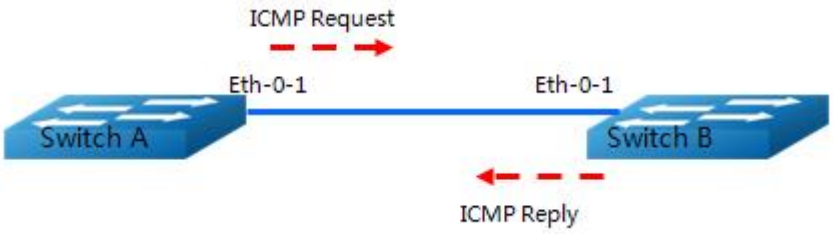


Figure 16-11 Topology

III. Configure VRF interface

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# ip vrf vpn1	Establish VRF entries
Switch(config-vrf)# exit	Exit VRF mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip vrf forwarding vpn1	Enable VRF forwarding table on the interface
Switch(config-if)# ip address 192.168.0.2/24	Configure IP address
Switch(config)# ip sla monitor 1	Create an IPSLA entry and enter IPSLA configuration mode
Switch(config-ipsla)# type icmp-echo 192.168.0.1	Define an ICMP echo action, and input its destination IP address
Switch(config-ipsla)# frequency 35	Set sending frequency
Switch(config-ipsla)# timeout 6	Set timeout
Switch(config-ipsla)# threshold 6000	Set threshold time
Switch(config-ipsla)# ttl 65	Set ttl
Switch(config-ipsla)# tos 1	Set tos
Switch(config-ipsla)# data-size 29	Set data size
Switch(config-ipsla)# data-pattern abababab	Set data pattern
Switch(config-ipsla)# fail-percent 90	Set fail percent
Switch(config-ipsla)# packets-per-test 4	Set packets per test for detecting
Switch(config-ipsla)# interval 9	Set probe interval
Switch(config-ipsla)# statistics packet 10	Set packet statistics
Switch(config-ipsla)# statistics test 3	Set to save recent test results

Switch(config-ipsla)# vrf vpn1	Apply VPN1
Switch(config-ipsla)# exit	Exit IPSLA mode
Switch(config)# ip sla monitor schedule 1	Enable IP SLA feature
Switch(config)# exit	Exit configuration mode

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# ip vrf vpn1	Establish VRF entries
Switch(config-vrf)# exit	Exit VRF mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip vrf forwarding vpn1	Enable VRF forwarding table on the interface
Switch(config-if)# ip address 192.168.0.1/24	Configure IP address

Ⅳ.Command validation

```
DUT1# sho ip sla monitor 1
Entry 1
   Type                 : Echo
   Admin state          : Disable
   Destination address  : 192.168.0.1
   Frequency            : 35s
   Timeout              : 6s
   Threshold            : 6000ms
   Interval             : 9s
   Packet per test      : 4
   TTL                  : 65
   TOS                  : 1
   Data Size            : 29 bytes
   Fail Percent         : 90%
   Packet Item Cnt      : 10
   Test Item Cnt        : 3
   Vrf                  : vpn1
   Return code          : Unknown
```

Ⅴ.Set layer 3 interface

Switch A

Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode

Switch(config-if)# ip address 192.168.0.2/24	Configure IP address
Switch(config)# ip sla monitor 1	Create an IPSLA entry and enter IPSLA configuration mode
Switch(config-ipsla)# type icmp-echo 192.168.0.1	Define an ICMP echo action, and input its destination IP address or host name
Switch(config-ipsla)# frequency 10	Set sending frequency
Switch(config-ipsla)# timeout 5	Set timeout
Switch(config-ipsla)# threshold 1	Set threshold time
Switch(config-ipsla)# exit	Exit IPSLA mode
Switch(config)# ip sla monitor schedule 1	Enable IP SLA feature
Switch(config)# exit	Exit configuration mode

Switch B

Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.1/24	Configure IP address

Ⅵ.Command validation

```
Switch# show ip sla monitor
Entry 1
   Type              : Echo
   Admin state                  : Enable
   Destination address          : 192.168.0.1
   Frequency                    : 10 seconds
   Timeout           : 5 seconds
   Threshold                    : 5 seconds
   Running Frequency            : 8 seconds
Return code                : OK
Switch# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.846 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.640 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.704 ms
```

Switch B

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode

Switch(config-if)# shutdown	Open the interface

```
Switch# show ip sla monitor
Entry 1
   Type                : Echo
   Admin state                 : Enable
   Destination address         : 192.168.0.1
   Frequency                   : 10 seconds
   Timeout             : 5 seconds
   Threshold                   : 5 seconds
   Running Frequency           : 9 seconds
   Running Timeout             : 4 seconds
   Running Threshold           : 4 seconds
Return code                 : Timeout
```

Ⅶ.Configure static routing port

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.2/24	Configure IP address
Switch(config)# ip sla monitor 2	Establish SLA entries
Switch(config-ipsla)# type icmp-echo 1.1.1.1	Define an ICMP echo action, and input its destination IP address or host name
Switch(config-ipsla)# frequency 10	Set sending frequency
Switch(config-ipsla)# timeout 5	Set timeout
Switch(config-ipsla)# threshold 1	Set threshold time
Switch(config-ipsla)# exit	Exit IPSLA mode
Switch(config)# ip sla monitor schedule 2	Enable IP SLA feature
Switch(config)# exit	Exit configuration mode

Ⅷ.Command validation

```
Switch# show ip sla monitor 2
Entry 2
   Type                : Echo
   Admin state                 : Enable
   Destination address         : 1.1.1.1
   Frequency                 : 10 seconds
   Timeout             : 5 seconds
   Threshold                   : 5 seconds
   Running Frequency           : 1 seconds
```

```
  Return code                    : Unreachable
Switch# ping 1.1.1.1
connect: Network is unreachable
```

Switch A

Switch#configure terminal	Enter configuration mode
Switch(config)# ip route 1.1.1.1/32 192.168.0.1	Configure static route

```
Switch# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.661 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.762 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=64 time=0.942 ms
Switch# show ip sla monitor 2
Entry 2
  Type                  : Echo
  Admin state                   : Enable
  Destination address           : 1.1.1.1
  Frequency             : 10 seconds
  Timeout               : 5 seconds
  Threshold                     : 5 seconds
  Running Frequency             : 8 seconds
  Return code                   : OK
```

16.10.2 Configure TRACK

I. Introduction

The monitor interface function of VRRP facilitates extending the backup function: provide the backup function in the case that the interface of a router of the backup team breaks down or other interfaces of the router (such as the interface connecting to uplink) become unavailable. When the interface accessing uplink breaks down, the backup team cannot perceive uplink failure. If the router is in master state in this case, the hosts in the LAN will become unable to access the external network. This problem can be solved by monitoring specific interface. When the interface accessing uplink is in down state, the router will actively lower its priority below the priority of other routers of the backup team, so that the router with the highest priority can become the master to take over forwarding action.

II. Topology

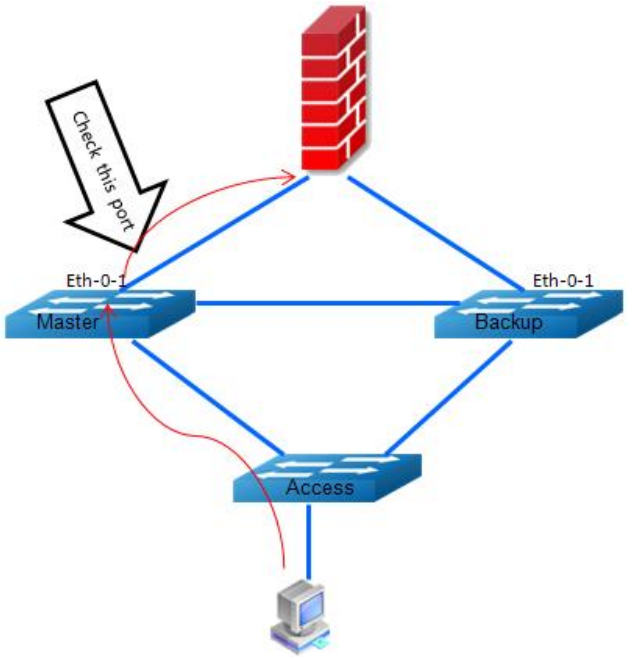


Figure 16-12 TRACK Topology

III. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# track 1 interface eth-0-1 linkstate	Establish track entries
Switch(config-track)# delay up 30	Time taken from down to up
Switch(config-track)# delay down 30	Time taken from up to down
Switch(config-track)#exit	Exit monitor mode
Switch(config)# exit	Exit configuration mode

IV. Command validation

Switch#show track

```
Track 2
   Type           : Interface Link state
   Interface      : eth-0-1
   State          : down
   Delay up       : 30 seconds
Delay down        : 30 seconds
```

Ⅰ.Topology

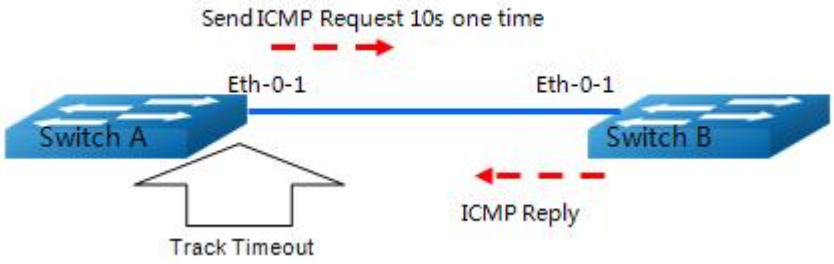


Figure 16-13 Topology

Ⅱ.Configuration

Switch A

Switch# configure terminal	Enter configuration mode
Switch(config)# track 1 rtr 1 reachability	Configure track reachability
Switch(config-track)# delay up 30	Time taken from down to up
Switch(config-track)# delay down 30	Time taken from up to down
Switch(config-track)#exit	Exit monitor mode
Switch(config)# exit	Exit configuration mode
Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.2/24	Configure IP address
Switch(config)# ip sla monitor 1	Establish SLA entries
Switch(config-ipsla)# type icmp-echo 192.168.0.1	Define an ICMP echo action, and input its destination IP address
Switch(config-ipsla)# frequency 10	Set sending frequency
Switch(config-ipsla)# timeout 5	Set timeout
Switch(config-ipsla)# threshold 1	Set threshold time
Switch(config-ipsla)# exit	Exit SLA mode
Switch(config)# ip sla monitor schedule 1	Enable IP SLA feature
Switch(config)# exit	Exit configuration mode

Switch B

Switch#configure terminal	Enter configuration mode

Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.1/24	Configure IP address

III .Validation

```
Switch#show track
Track 1
   Type                : Response Time Reporter(RTR) Reachability
   RTR entry number    : 1
   State               : up
   Delay up            : 30 seconds
Delay down             : 30 seconds
```

I. Topology

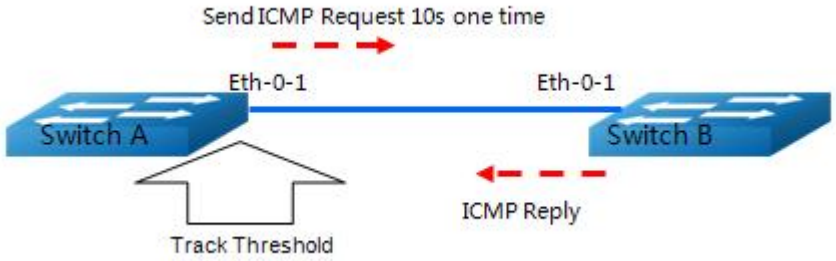


Figure 16-14 Topology

II. Configuration

Switch A

Command	Description
Switch#configure terminal	Enter configuration mode
Switch(config)# track 1 rtr 1 state	Configure track state
Switch(config-track)# delay up 30	Time taken from down to up
Switch(config-track)# delay down 30	Time taken from up to down
Switch(config-track)#exit	Exit track mode
Switch(config)# exit	Exit configuration mode
Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.2/24	Configure IP address
Switch(config)# ip sla monitor 1	Establish IP SLA entries
Switch(config-ipsla)# type icmp-echo 192.168.0.1	Define IP SLA protocol type

Command	Description
Switch(config-ipsla)# frequency 10	Set sending frequency
Switch(config-ipsla)# timeout 5	Set timeout
Switch(config-ipsla)# threshold 1	Set threshold time
Switch(config-ipsla)# exit	Exit IPSLA mode
Switch(config)# ip sla monitor schedule 1	Enable IP SLA monitor
Switch(config)# exit	Exit configuration mode

Switch B

Command	Description
Switch#configure terminal	Enter configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ip address 192.168.0.1/24	Configure IP address

Ⅳ.Command validation

```
Switch# show track
Track 1
   Type                 : Response Time Reporter(RTR) State
   RTR entry number   : 1
   State                : up
   Delay up             : 30 seconds
Delay down              : 30 seconds
```

16.10.3 Configure Track BFD

Topology

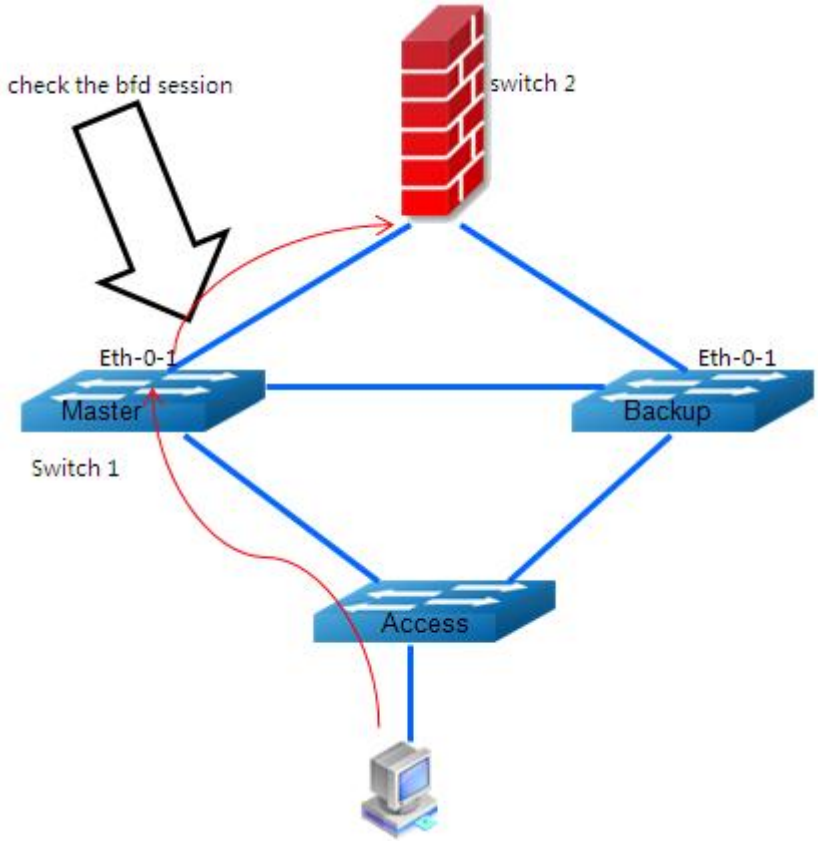


Figure 16-15 VRRP Track BFD Topology

Configuration

Configure vrrp track bfd following the steps listed in the table below:

Switch1 Configuration

Switch1# configure terminal	Enter configuration mode
Switch 1(config)# interface eth-0-1	Enter port configuration mode
Switch 1(config-if)# no switchport	Set the interface as layer3 interface
Switch 1(config-if)# no shutdown	Enable the interface
Switch 1(config-if)# ip address 9.9.9.1/24	Configure IP address
Switch 1(config-if)# quit	Exit interface mode
Switch1(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.2	Create track object of bfd session

Switch1(config-track)# delay up 30	Time taken from down to up
Switch1(config-track)# delay down 30	Time taken from up to down
Switch1(config-track)# exit	Exit track mode
Switch1(config)# exit	Exit configuration mode

Switch2 Configuration

Switch2# configure terminal	Enter configuration mode
Switch2(config)# interface eth-0-1	Enter port configuration mode
Switch2 (config-if)# no switchport	Set the interface as layer3 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 9.9.9.2/24	Configure IP address
Switch2(config-if)# quit	Exit interface mode
Switch2(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.1	Create track object of bfd session
Switch1(config-track)# delay up 30	Time taken from down to up
Switch1(config-track)# delay down 30	Time taken from up to down
Switch1(config-track)# exit	Exit track mode
Switch1(config)# exit	Exit configuration mode

Command Validation

Use the following command to show track bfd configuration:

```
Switch #show track
Track 1
   Type                : BFD state
   Source interface    : eth-0-1
   Destination IP      : 9.9.9.2
   BFD Local discr     : 1
   State               : up
Switch2 # show track
Track 1
   Type                : BFD state
   Source interface    : eth-0-1
   Destination IP      : 9.9.9.1
   BFD Local discr     : 1
   State               : up
```

16.10.4 Configure VRRP TRACK

I. Topology

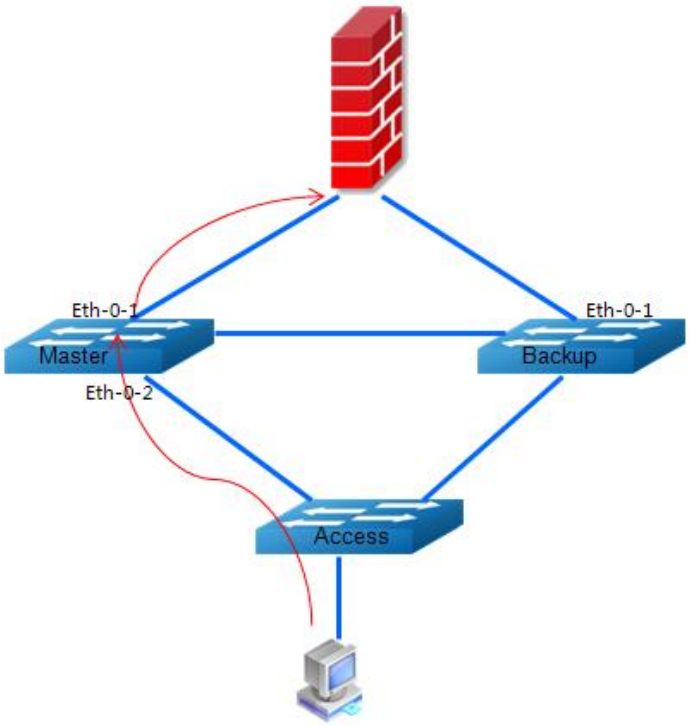


Figure 16-16 Topology

II. Configuration

Switch# configure terminal	Enter configuration mode
Switch(config)# track 1 interface eth-0-1 linkstate	Configure track entries
Switch(config-track)#exit	Exit track mode
Switch(config)# router vrrp 1	Establish VRRP entries
Switch(config-router)# track 1 decrement 30	Establish VRRP rules
Switch(config-router)# exit	Exit routing mode
Switch(config)# exit	Exit configuration mode

III. Command validation

```
Switch# show vrrp
VRID <1>
 State          : Master
 Virtual IP     : 172.16.10.100(Not IP owner)
 Interface      : eth-0-2
 VMAC           : 0000.5e00.0101
 Advt timer     : 1
```

```
Preempt mode    : TRUE
Auth type       : NONE
Conf pri        : Unset      Run pri  : 70
Track Object    : 1
Delta pri       : 30
Master router ip  : 172.16.10.1
Master priority   : 70
Master advt timer  : 1
Master down timer  : 4
Learn master mode  : FALSE
```

16.10.5 Configure Static Route Track

I. Topology

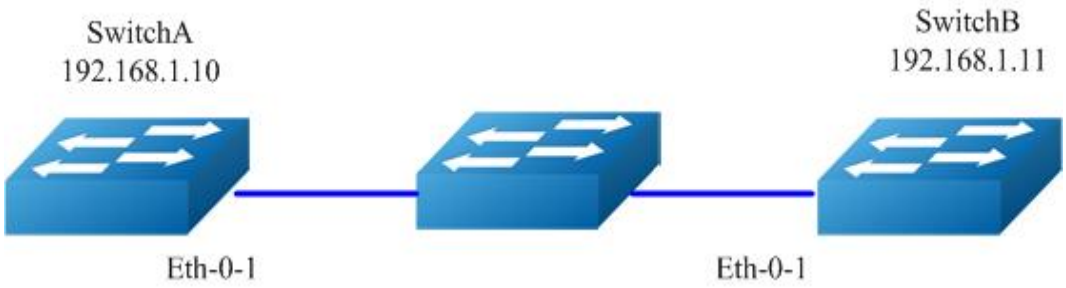


Figure 16-17 Static Routing Track Topology

II. Configuration

Switch A

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# ip address 192.168.1.10/24	Configure interface IP address
Switch(config-if)# exit	Exit interface mode
Switch(config)# ip sla monitor 1	Create an IP SLA entry and enter IP SLA configuration mode
Switch(config-ipsla)# type icmp-echo 192.168.1.11	Define an ICMP echo action, and input its destination IP address
Switch(config-ipsla)# exit	Exit IP SLA configuration mode
Switch(config)# ip sla monitor schedule 1	Enable IP SLA feature
Switch(config)# track 1 rtr 1 reachability	Create track entry and enter track configuration mode
Switch(config-track)#exit	Exit track configuration mode

Switch(config)#ip route 10.10.10.0/24 192.168.1.11 track 1	Configure static route, and assign track entry
Switch(config)# exit	Exit global configuration mode

Switch B

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# no switchport	Set the interface as Layer 3 interface
Switch(config-if)# no shutdown	Open the interface
Switch(config-if)# ip address 192.168.1.11/24	Configure interface IP address

III. Command validation

```
Switch# show ip sla monitor 1
Entry 1
   Type                  : Echo
   Admin state           : Enable
   Destination address   : 192.168.1.11
   Frequency             : 60 seconds
   Timeout               : 5 seconds
   Threshold             : 5 seconds
   Running Frequency     : 49 seconds
Return code              : OK
Switch# show track 1
Track 1
   Type                  : Response Time Reporter(RTR) Reachability
   RTR entry number      : 1
   State                 : up
Switch# show ip route static
S       10.10.10.0/24 [1/0] via 192.168.1.11, eth-0-1
```

Switch B

Switch# configure terminal	Enter global configuration mode
Switch(config)# interface eth-0-1	Enter interface configuration mode
Switch(config-if)# shutdown	Shut down the interface

```
Switch# show ip sla monitor 1
Entry 1
   Type                  : Echo
   Admin state           : Enable
   Destination address   : 192.168.1.11
   Frequency             : 60 seconds
   Timeout               : 5 seconds
```

```
    Threshold                : 5 seconds
    Running Frequency    : 8 seconds
Return code                : Timeout
Switch# show track 1
Track 1
    Type                     : Response Time Reporter(RTR) Reachability
    RTR entry number    : 1
    State                    : down
Switch# show ip route static
Switch#
```

16.11 IP BFD Configuration

16.11.1 Introduction

As the requirement for network reliability becomes increasingly high, the ability of quickly locating and switching to backup link to guarantee network smoothness becomes more and more important. Many hardware or software don't have this ability, such as Ethernet. Some hardware or software are unable to perform path detection. For example, forwarding engine or interface is unable to perform end-to-end detection.

The current network usually adopts the slow Hello mechanism. Especially for routing protocol, the detection time is very long without the support of hardware. As data rate increases, long time for fault induction means a lot of data loss, and it is unable to detect the link state of nodes not allowing routing protocol. Meanwhile, the existing IP networks are unable to perform faster-than-second intermittent fault correcting, and the conventional routing architecture only has limited ability of accurate fault detection for real-time application (such as voice).

BFD provides a quick underloading solution to link status detection. BFD is capable of fault detection on channels of any type between systems, including physical link, virtual circuit, tunnel, MPLS LSP, multi-hop routing channel, and undirect channel.

16.11.2 Limit

If a CFM mep is configured and LM is enabled on the physical interface, and IP BFD is configured on the vlan interface and the physical interface is a member of the vlan interface, the IP BFD cannot work normally. IP BFD should be able to work normally when LM is disabled.

16.11.3 Topology

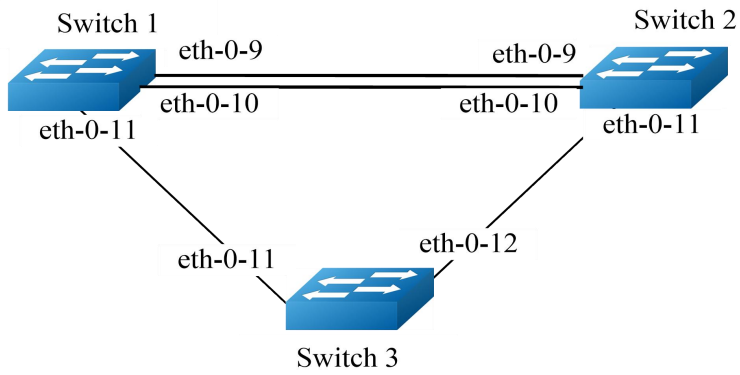


Figure 16-18 Basic Configuration of IP BFD Single-hop Session

16.11.4 Configuration

The topology contains three BFD sessions, one is based on static configuration and associated with static route, one is OSPF-based, and the last one is linkage between bfd and vrrp.

Switch1 Configuration

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# interface eth-0-9	Enter interface eth-0-9 configuration mode
Switch1 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# ip address 9.9.9.1/24	Configure interface IP address
Switch1(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	Configure interface BFD mintx minrx, and detection multiplier
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# interface eth-0-10	Enter interface eth-0-10 configuration mode
Switch1 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# ip address 10.10.10.1/24	Configure interface IP address
Switch1(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	Configure interface BFD mintx minrx, and detection multiplier
Switch1(config-if)# ip ospf bfd	Enable OSPF-based BFD
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# router ospf	Enter OSPF mode

Switch1 (config-router)# network 10.10.10.0/24 area 0	Configure OSPF network segment
Switch1 (config-router)# exit	Exit OSPF mode
Switch1(config)# interface eth-0-11	Enter interface mode
Switch1 (config-if)# no switchport	Set the interface as layer3 interface
Switch1(config-if)# ip address 11.11.11.1/24	Set IP address
Switch 1(config-if)#exit	Exit interface mode
Switch1 (config)#router vrrp 1	Create virtual router group 1
Switch(config-router)# virtual-ip 11.11.11.100	Set virtual IP address.
Switch 1(config-router)#interface eth-0-11	Configure application port of VRRP group
Switch 1(config-router)# bfd 11.11.11.2	Configure BFD session
Switch1(config-router)# enable	Enable VRRP group 1
Switch1(config)# bfd test peer-ip 9.9.9.2 interface eth-0-9 auto	Create bfd session
Switch1(config)# ip route 1.1.1.0/24 9.9.9.2 bind bfd test	Configure static route and make association with bfd session
Switch1 (config)# end	Exit global configuration mode

Switch2 Configuration

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-9	Enter interface eth-0-9 configuration mode
Switch2 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 9.9.9.2/24	Configure interface IP address
Switch2(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	Configure interface BFD mintx minrx, and detection multiplier
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-10	Enter interface eth-0-10 configuration mode
Switch2 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 10.10.10.2/24	Configure interface IP address

Switch2(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	Configure interface BFD mintx minrx, and detection multiplier
Switch2(config-if)# ip ospf bfd	Enable OSPF-based BFD
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# router ospf	Enter OSPF mode
Switch2 (config-router)# network 10.10.10.0/24 area 0	Configure OSPF network segment
Switch2 (config-router)# exit	Exit OSPF mode
Switch2(config)# interface eth-0-11	Enter interface mode
Switch2 (config-if)# no switchport	Set the interface as layer3 interface
Switch2(config-if)# ip address 11.11.11.2/24	Set IP address
Switch2(config-if)# exit	Exit interface mode
Switch2 (config)#router vrrp 1	Create virtual router group 1
Switch2 (config-router)#virtual-ip 11.11.11.100	Set virtual IP address.
Switch2 (config-router)#interface eth-0-11	Configure application port of VRRP group
Switch2 (config-router)# bfd 11.11.11.1	Configure BFD session
Switch2(config-router)# enable	Enable VRRP group 1
Switch1(config)# bfd test peer-ip 9.9.9.1 interface eth-0-9 auto	Create bfd session
Switch2(config)# ip route 2.2.2.0/24 9.9.9.1 bind bfd test	Configure static route and make association with bfd session
Switch2 (config)# end	Exit global configuration mode

Switch3 Configuration

Switch3# configure terminal	Enter global configuration mode
Switch3(config)# interface eth-0-11	Enter interface eth-0-11 configuration mode
Switch3(config-if)# no shutdown	Enable the interface
Switch 3(config-if)#exit	Exit interface mode
Switch3(config)# interface eth-0-12	Enter interface eth-0-12 configuration mode
Switch3(config-if)# no shutdown	Enable the interface
Switch 3(config-if)#exit	Exit interface mode

16.11.5 Command Validation

Use command “show bfd session” to check configuration result, as below.

```
Switch1# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
SD: Static Discriminator.  DD: Dynamic Discriminator
A: Admin down.    D:down.    I:init.    U:up.
=================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr       vrf
1    1    S-DD U    00:01:05   9.9.9.2         default
2    2    S-DD U    00:00:25   10.10.10.2      default
3    3    S-DD U    00:00:25   11.11.11.2      default
Number of Sessions:   3
Switch2# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
SD: Static Discriminator.  DD: Dynamic Discriminator
A: Admin down.    D:down.    I:init.    U:up.
=================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr       vrf
1    1    S-DD    U   00:01:27   9.9.9.1       default
2    2    S-DD    U   00:00:46   10.10.10.1    default
3    3    S-DD    U   00:00:25   11.11.11.3    default
Number of Sessions:   3
```

16.11.6 Multi-hop Topology

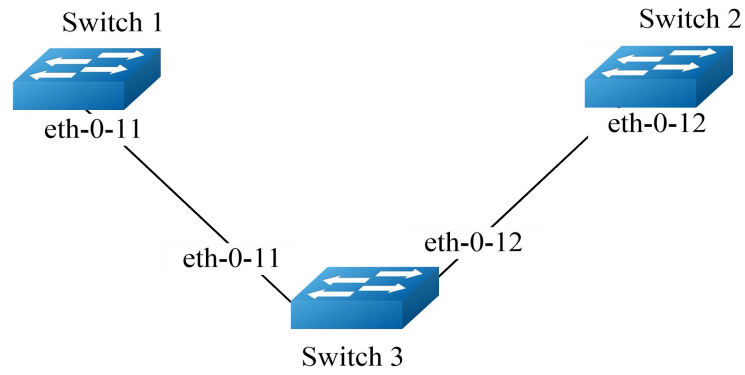


Figure 16-19 Basic Configuration of IP BFD Multi-hop Session

16.11.7 Multi-hop Configuration

The topology contains multi-hop bfd session statically configured and association with static route.

Switch1 Configuration

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# interface eth-0-11	Enter interface eth-0-11 configuration mode
Switch1 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# ip address 11.11.11.1/24	Configure interface IP address
Switch1(config-if)# exit	Exit interface mode
Switch1(config)#ip route 12.12.12.2/24 11.11.11.2	Configure static route to switch 3
Switch1(config)# bfd test peer-ip 12.12.12.2/24 source 11.11.11.1 local 10 remote 20	Configure static multi-hop bfd and specify local identifier
Switch1(config)# ip route 192.168.1.1/24 12.12.12.2 bind bfd test	Associate bfd with a static route

Switch2 Configuration

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-11	Enter interface eth-0-11 configuration mode
Switch2 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 11.11.11.2/24	Configure interface IP address
Switch2(config-if)# exit	Exit interface mode
Switch2(config)# interface eth-0-12	Enter interface eth-0-12 configuration mode
Switch2 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 12.12.12.1/24	Configure interface IP address
Switch2(config-if)# exit	Exit interface mode

Switch3 Configuration

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# interface eth-0-12	Enter interface eth-0-11 configuration mode

Switch2 (config-if)# no switchport	Set the interface as non-layer2 interface
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# ip address 12.12.12.2/24	Configure interface IP address
Switch2(config-if)# exit	Exit interface mode
Switch2(config)#ip route 11.11.11.1/24 12.12.12.1	Configure static route to switch 1
Switch2(config)#bfd test peer-ip 11.11.11.1 source-ip 12.12.12.2 local 20 remote 10	Configure static multi-hop bfd
Switch2(config)# ip route 2.2.2.2/24 11.11.11.1 bind bfd test	Configure static route binding bfd

16.11.8 Multi-hop Command Validation

Use command “show bfd session” to check configuration result, as below.

```
Switch1# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
SD: Static Discriminator.  DD: Dynamic Discriminator
A: Admin down.    D:down.    I:init.    U:up.
================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr       vrf
10   20   S-SD U    00:01:27   12.12.12.2      default
Switch1# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
SD: Static Discriminator.  DD: Dynamic Discriminator
A: Admin down.    D:down.    I:init.    U:up.
================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr       vrf
20   10   S-SD U    00:01:27   11.11.11.1      default
```

16.12 VARP Configuration

16.12.1 Introduction

Virtual ARP allows multiple switches to route messages according to a same destination MAC address simultaneously. Every switch will be configured with a same virtual MAC address to match the virtual ip address of VLAN interface. Since virtual ARP works in active-active mode without additional cost, virtual ARP is superior to VRRP in the application environment of MLAG.

For ARP and GARP requests from a virtual IP address, virtual ARP will give a response with a virtual MAC address. The virtual MAC address will appear in the ingress messages only, and not appear in the source IP field of egress messages.

16.12.2 Topology

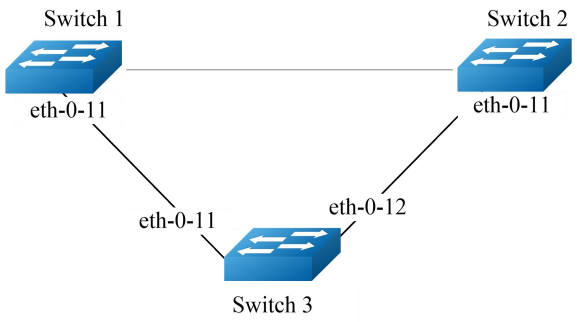


Figure 16-20 VARP & MLAG Topology

16.12.3 Configuration

Configure VARP.

Switch1 Configuration

Switch1# configure terminal	Enter global configuration mode
Switch1(config)# ip virtual-router mac a.a.a	Configure virtual MAC address
Switch1 (config)# vlan database	Enter VLAN configuration mode
Switch1 (config-vlan)# vlan 2	Create VLAN 2
Switch1(config-vlan)# exit	Exit VLAN configuration mode
Switch1(config)# interface eth-0-11	Enter interface eth-0-11 configuration mode
Switch1(config-if)# switchport access vlan 2	Add the interface into vlan 2
Switch1(config-if)# no shutdown	Enable the interface
Switch1(config-if)# interface vlan 2	Enter vlan2 interface configuration mode
Switch1(config-if)# ip address 10.10.10.1/24	Configure IP address
Switch1(config-if)# ip virtual-router address 10.10.10.254	Configure virtual IP address
Switch1(config-if)# end	Exit interface configuration mode

Switch2 Configuration

Switch2# configure terminal	Enter global configuration mode
Switch2(config)# ip virtual-router mac a.a.a	Configure virtual MAC address
Switch2 (config)# vlan database	Enter VLAN configuration mode
Switch2 (config-vlan)# vlan 2	Create VLAN 2
Switch2(config-vlan)# exit	Exit VLAN configuration mode
Switch2(config)# interface eth-0-11	Enter interface eth-0-11 configuration mode
Switch2(config-if)# switchport access vlan 2	Add the interface into vlan 2
Switch2(config-if)# no shutdown	Enable the interface
Switch2(config-if)# interface vlan 2	Enter vlan2 interface configuration mode
Switch2(config-if)# ip address 10.10.10.2/24	Configure IP address
Switch2(config-if)# ip virtual-router address 10.10.10.254	Configure virtual IP address
Switch2(config-if)# end	Exit interface configuration mode

16.12.4 Command Validation

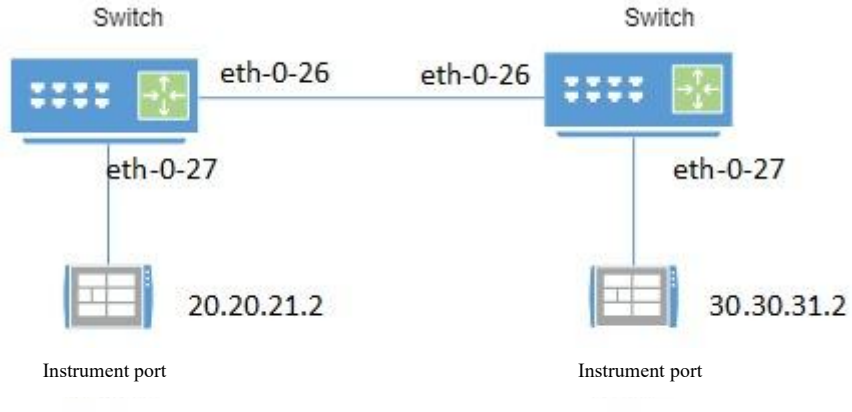
The show results of ARP are as below:

```
Switch1# show ip arp
 Protocol   Address         Age (min)  Hardware Addr   Interface
 Internet   10.10.10.1          -   cef0.12da.8100  vlan2
 Internet   10.10.10.254        -   000a.000a.000a  vlan2
Switch2#  show ip arp
 Protocol   Address         Age (min)  Hardware Addr   Interface
 Internet   10.10.10.2          -   66d1.4c26.e100  vlan2
 Internet   10.10.10.254        -   000a.000a.000a  vlan2
```

17 EVPN Configuration Guide

17.1 Naddod Equipment Test

17.1.1 Topology



17.1.2 DUT1 Configuration

PS: Border, an external route is needed (type5)
DUT1:

DUT1# configure terminal	Enter global configuration mode
DUT1(config)# ip vrf test	Create vrf
DUT1(config-vrf)# vni 50000 l3	Create L3 VNI
DUT1(config-vrf)# rd 1:50000	Configure L3 VNI RD
DUT1(config-vrf)#route-target both 50:50000	Configure L3 VNI RT
DUT1(config-vrf)# exit	Go back to global configuration mode
DUT1 (config)# vlan database	Enter VLAN configuration mode
DUT1(config-vlan)# vlan 20,30,50	Create VLAN 20,50
DUT1(config-vlan)# vlan 20 overlay enable	Enable vlan 20 overlay function
DUT1(config-vlan)# vlan 30 overlay enable	Enable vlan 30 overlay function
DUT1(config-vlan)# vlan 50 overlay enable	Enable vlan 50 overlay function

DUT1(config-vlan)# exit	Go back to global configuration mode
DUT1(config)# overlay	Enter overlay configuration mode
DUT1(config-overlay)# source 1.1.1.1	Configure source vtep address of vxlan
DUT1(config-overlay)# vtep reachability protocol bgp	Enable dynamic VxLAN tunnel construction function
DUT1(config-overlay)# vlan 20 vni 20000	Configure vlan and vni mapping
DUT1(config-overlay)# vlan 30 vni 30000	Configure vlan and vni mapping
DUT1(config-overlay)# vlan 50 vni 50000	Configure vlan and vni mapping
DUT1(config- overlay)# exit	Go back to global configuration mode
DUT1(config)# evpn	Enter EVPN configuration mode
DUT1(config-evpn)# vni 20000	Create L2 VNI
DUT1(config-evi)# rd auto	Automatically generate RD
DUT1(config-evi)# route-target both auto	Automatically generate RT
DUT1(config-evi)# exit	Go back to EVPN configuration mode
DUT1(config-evpn)# vni 30000	Create EVPN instance and enter EVPN instance configuration mode
DUT1(config-evi)# rd auto	Automatically generate RD
DUT1(config-evi)# route-target both auto	Automatically generate RT
DUT1(config-evi)# exit	Go back to EVPN configuration mode
DUT1(config-evpn)# exit	Go back to global configuration mode
DUT1(config)# interface eth-0-26	Enter interface eth-0-26 configuration
DUT1 (config-if)# no switchport	Change into routed port
DUT1(config-if)# ip address 26.26.26.1/24	Configure IP address
DUT1(config-if)# overlay uplink enable	Enable overlay uplink port
DUT1(config-if)# exit	Go back to global configuration mode
DUT1(config)# interface eth-0-27	Enter interface eth-0-27 configuration
DUT1(config-if)# switchport access vlan 20	Add the interface into vlan 20
DUT1(config)# interface vlan 20	Enter vlanif 20 configuration
DUT1(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT1(config-if)#overlay distributed-gateway enable	Enable distributed gateway
DUT1(config-if)# ip address 20.20.20.1/24	Configure interface vlanif 20 address
DUT1(config-if)# ip virtual-router address 20.20.21.1/24	Configure virtual IP address of interface vlanif
DUT1(config-if)#overlay host-collect enable	Enable host-collect function
DUT1(config-if)# exit	Go back to global configuration mode

DUT1(config)# interface vlan 30	Enter vlanif 30 configuration
DUT1(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT1(config-if)#overlay distributed-gateway enable	Enable distributed gateway
DUT1(config-if)# ip address 30.30.30.1/24	Configure interface vlanif 30 address
DUT1(config-if)# ip virtual-router address 30.30.31.1/24	Configure virtual IP address of interface vlanif
DUT1(config-if)#overlay host-collect enable	Enable host-collect function
DUT1(config-if)# exit	Go back to global configuration mode
DUT1(config)# interface vlan 50	Enter vlanif 50 configuration
DUT1(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT1(config-if)# exit	Go back to global configuration mode
DUT1(config)# interface loopback 0	Create loopback port
DUT1(config-if)# ip address 1.1.1.1/32	Configure IP address
DUT1(config-if)# exit	Go back to global configuration mode
DUT1(config)# router bgp 100	Create BGP 100 and enter routing configuration mode
DUT1(config)# bgp router-id 1.1.1.1	Configure BGP router-id
DUT1(config-router)# neighbor 2.2.2.2 remote-as 100	Create IGBP neighbor
DUT1(config-router)# neighbor 2.2.2.2 update-source loopback0	Assign update source port
DUT1(config- router)# address-family l2vpn evpn	Enter EVPN address family configuration mode
DUT1(config- router-af)# neighbor 2.2.2.2 activate	Activate exchanging routing information with neighbor
DUT1(config- router-af)# exit	Go back to routing configuration mode
DUT1(config-router)# address-family ipv4 vrf test	Enter IPV4 VRE address family configuration mode
DUT1(config-router-af)# redistribute connected	Configure routing redistribution
DUT1(config-router-af)# advertise l2vpn	Configure introducing routing redistribution into EVPN
DUT1(config- router-af)# exit	Go back to routing configuration mode
DUT1 (config-router)# exit	Go back to global configuration mode
DUT1(config)#ip route 2.2.2.0/24 26.26.26.2	Configure static route

DUT1(config)#ip virtual-router mac 0001.0001.0001	Configure virtual mac

17.1.3 DUT1 Configuration

DUT2:

DUT2# configure terminal	Enter global configuration mode
DUT2(config)# ip vrf test	Create vrf
DUT2(config-vrf)# vni 50000 l3	Create L3 VNI
DUT2(config-vrf)# rd 1:50000	Configure L3 VNI RD
DUT2(config-vrf)#route-target both 50:50000	Configure L3 VNI RT
DUT2 (config)# vlan database	Enter VLAN configuration mode
DUT2(config-vlan)# vlan 20,30,50	Create VLAN 20,50
DUT2(config-vlan)# vlan 20 overlay enable	Enable vlan 20 overlay function
DUT2(config-vlan)# vlan 30 overlay enable	Enable vlan 30 overlay function
DUT2(config-vlan)# vlan 50 overlay enable	Enable vlan 50 overlay function
DUT2(config-vlan)# exit	Go back to global configuration mode
DUT2(config)# overlay	Enter overlay configuration mode
DUT2(config-overlay)# source 2.2.2.2	Configure source vtep address of vxlan
DUT2(config-overlay)# vtep reachability protocol bgp	Enable dynamic VxLAN tunnel construction function
DUT2(config-overlay)# vlan 20 vni 20000	Configure vlan and vni mapping
DUT2(config-overlay)# vlan 30 vni 30000	Configure vlan and vni mapping
DUT2(config-overlay)# vlan 50 vni 50000	Configure vlan and vni mapping
DUT2(config- overlay)# exit	Go back to global configuration mode
DUT2(config)# evpn	Enter EVPN configuration mode
DUT2(config-evpn)# vni 20000	Create EVPN instance and enter EVPN instance configuration mode
DUT2(config-evi)# rd auto	Automatically generate RD
DUT2(config-evi)# route-target both auto	Automatically generate RT
DUT2(config-evi)# exit	Go back to EVPN configuration mode
DUT2(config-evpn)# vni 30000	Create EVPN instance and enter EVPN instance configuration mode
DUT2(config-evi)# rd auto	Automatically generate RD
DUT2(config-evi)# route-target both auto	Automatically generate RT
DUT2(config-evi)# exit	Go back to EVPN configuration mode

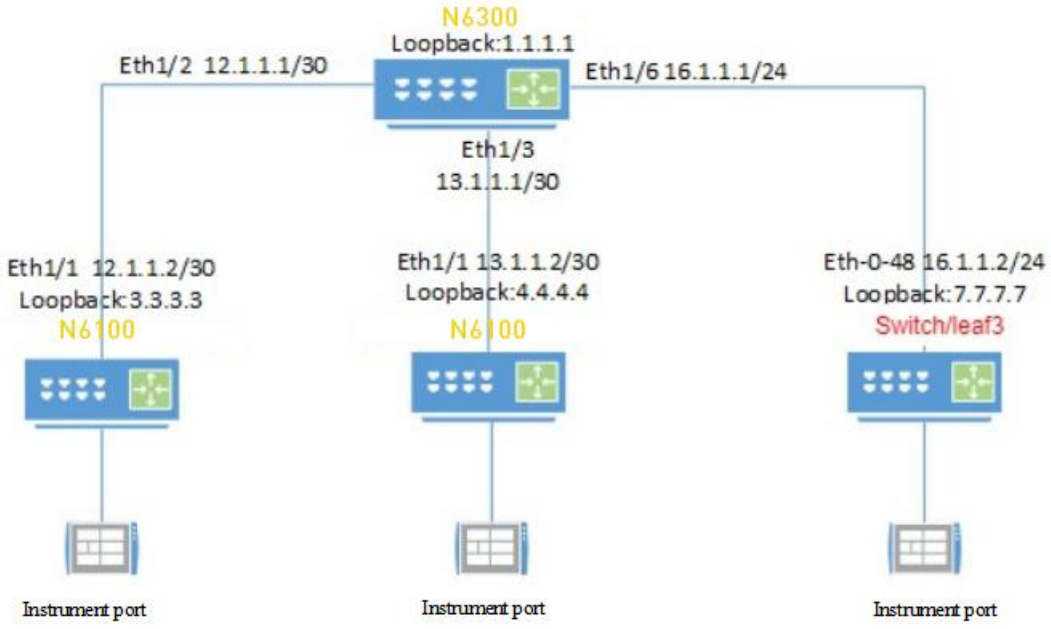
DUT2(config-evpn)# exit	Go back to global configuration mode
DUT2(config)# interface eth-0-26	Enter interface eth-0-26 configuration
DUT2 (config-if)# no switchport	Change into routed port
DUT2(config-if)# ip address 26.26.26.1/24	Configure IP address
DUT2(config-if)# overlay uplink enable	Enable overlay uplink port
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# interface eth-0-27	Enter interface eth-0-27 configuration
DUT2(config-if)# switchport access vlan 30	Add the interface into vlan 30
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# interface vlan 20	Enter vlanif 20 configuration
DUT2(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT2(config-if)#overlay distributed-gateway enable	Enable distributed gateway
DUT2(config-if)# ip address 20.20.20.1/24	Configure interface vlanif 20 address
DUT2(config-if)# ip virtual-router address 20.20.21.1/24	Configure virtual IP address of interface vlanif
DUT2(config-if)#overlay host-collect enable	Enable host-collect function
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# interface vlan 30	Enter vlanif 30 configuration
DUT2(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT2(config-if)#overlay distributed-gateway enable	Enable distributed gateway
DUT2(config-if)# ip address 30.30.30.1/24	Configure interface vlanif 30 address
DUT2(config-if)# ip virtual-router address 30.30.31.1/24	Configure virtual IP address of interface vlanif
DUT2(config-if)#overlay host-collect enable	Enable host-collect function
DUT2(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# interface vlan 50	Enter vlanif 50 configuration
DUT2(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# interface loopback 0	Create loopback port
DUT2(config-if)# ip address 2.2.2.2/32	Configure IP address
DUT2(config-if)# exit	Go back to global configuration mode
DUT2(config)# router bgp 100	Create BGP 100 and enter routing configuration mode

DUT2(config)# bgp router-id 2.2.2.2	Configure BGP router-id
DUT2(config-router)# neighbor 1.1.1.1 remote-as 100	Create IGBP neighbor
DUT2(config-router)# neighbor 1.1.1.1 update-source loopback0	Assign update source port
DUT2(config- router)# address-family l2vpn evpn	Enter EVPN address family configuration mode
DUT2(config- router-af)# neighbor 1.1.1.1 activate	Activate exchanging routing information with neighbor
DUT2(config- router-af)# exit	Go back to routing configuration mode
DUT2 (config-router)# exit	Go back to global configuration mode
DUT2(config)#ip route 1.1.1.0/24 26.26.26.1	Configure static route
DUT2(config)#ip virtual-router mac 0001.0001.0001	Configure virtual mac

17.2 Naddod Equipment Docking Test

17.2.1 Test Case with RR

17.2.2 Topology



N6300 and N6100 are Naddod equipment,N6300 is taken as route reflector, and switch is an Naddod device.

17.2.3 RR Configuration

RR# configure terminal	Enter global configuration mode
RR(config)# nv overlay evpn	Enable EVPN control plane for VXLAN
RR(config)# feature bgp	Enable bgp
RR(config)# feature ospf	Enable ospf
RR(config)# feature interface-vlan	Enable interface vlan
RR(config)# feature vn-segment-vlan-based	Enable VLAN-based VXLAN
RR(config)# feature nv overlay	Enable vxlan
RR(config)# router ospf 1	Enable ospf
RR(config)# interface ethernet 1/2	Enter interface eth1/ 2 configuration
RR(config)# no switchport	Change into routed port
RR(config-if)# ip address 12.1.1.1/30	Configure IP address
RR(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
RR(config-if)#no shutdown	Turn on the interface
RR(config-if)# exit	Go back to global configuration mode
RR(config)# interface ethernet 1/3	Enter interface eth1/ 3 configuration
RR(config)# no switchport	Change into routed port
RR(config-if)# ip address 13.1.1.1/30	Configure IP address
RR(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
RR(config-if)#no shutdown	Turn on the interface
RR(config-if)# exit	Go back to global configuration mode
RR(config)# interface ethernet 1/6	Enter interface eth1/ 3 configuration
RR(config)# no switchport	Change into routed port
RR(config-if)# ip address 16.1.1.1/30	Configure IP address
RR(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
RR(config-if)#no shutdown	Turn on the interface
RR(config-if)# exit	Go back to global configuration mode
RR(config)# interface loopback 1	Create loopback port
RR(config-if)# ip address 1.1.1.1/32	Configure IP address
RR(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
RR(config-if)# exit	Go back to global configuration

	mode
RR(config)# router bgp 65101	CreateBGP 65101 and enter routing configuration mode
RR(config-router)# router-id 1.1.1.1	Configure router ID
RR(config- router)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
RR(config-router)# address-family l2vpn evpn	Enter 12vpn evpn address family configuration mode
RR(config- router-af)# retain route-target all	Retain route target attribute
RR(config-router)# template peer VTEP	iBGP peer template
RR(config-router-neighbor)# remote-as 65101	Neighbor AS
RR(config-router-neighbor)# update-source loopback1	Update source port
RR(config-router-neighbor)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
RR(config-router-neighbor-af)# send-community	Send community name in address family
RR(config-router-neighbor-af)# send-community extended	Send community extended name in address family
RR(config-router-neighbor-af)# route-reflector-client	Enable RR
RR(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
RR(config-router-neighbor)# address-family l2vpn evpn	Enter 12vpn evpn address family configuration mode
RR(config-router-neighbor-af)# send-community	Send community name in address family
RR(config-router-neighbor-af)# send-community extended	Send community extended name in address family
RR(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
RR(config-router-neighbor)# exit	Go back to routing configuration mode
RR(config-router)# neighbor 3.3.3.3	Create IGBP neighbor
RR(config-router-neighbor)# inherit peer VTEP	Establish neighbor with peer template
RR(config-router-neighbor)# exit	Go back to routing configuration

	mode
RR(config-router)# neighbor 4.4.4.4	Create IGBP neighbor
RR(config-router-neighbor)# inherit peer VTEP	Establish neighbor with peer template
RR(config-router-neighbor)# exit	Go back to routing configuration mode
RR(config-router)# neighbor 7.7.7.7	Create IGBP neighbor
RR(config-router-neighbor)# inherit peer VTEP	Establish neighbor with peer template

17.2.4 Leaf1 Configuration

LEAF1# configure terminal	Enter global configuration mode
LEAF1(config)# nv overlay evpn	Enable EVPN control plane for VXLAN
LEAF1(config)# feature bgp	Enable bgp
LEAF1(config)# feature ospf	Enable ospf
LEAF1(config)# feature interface-vlan	Enable interface vlan
LEAF1(config)# feature vn-segment-vlan-based	Enable VLAN-based VXLAN
LEAF1(config)# feature nv overlay	Enable vxlan
LEAF1(config)# router ospf 1	Enable OSPF protocol
LEAF1(config)# vlan 100,200,300	Create VLAN
LEAF1(config-vlan)# exit	Go back to global configuration mode
LEAF1(config)# vlan 100	Enter VLAN 100
LEAF1(config-vlan)# vn-segment 100	Create VLAN-VNI mapping
LEAF1(config-vlan)# exit	Go back to global configuration mode
LEAF1(config)# vlan 200	Enter VLAN 200
LEAF1(config-vlan)# vn-segment 200	Create VLAN-VNI mapping
LEAF1(config-vlan)# exit	Go back to global configuration mode
LEAF1(config)# vlan 300	Enter VLAN 300
LEAF1(config-vlan)# vn-segment 300	Create VLAN-VNI mapping
LEAF1(config)#vrf context evpn-tenant-1	Create vrf

LEAF1(config-vrf)# vni 300	Create L3 VNI
LEAF1(config-vrf)# rd 1:300	Configure RD
LEAF1(config-vrf)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
LEAF1(config-vrf-af-ipv4)#route-target import 300:300	Configure RT
LEAF1(config-vrf-af-ipv4)#route-target export 300:300	Configure RT
LEAF1(config-vrf-af-ipv4)# interface Vlan100	Enter interface vlan
LEAF1(config-if)# no shutdown	Turn on the interface
LEAF1(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF1(config-if)# ip address 10.1.1.1/24	Configure IP address
LEAF1(config-if)#fabric forwarding mode anycast-gateway	Enable distributed anycast gateway
LEAF1(config-if)# interface Vlan200	Enter interface vlan
LEAF1(config-if)# no shutdown	Turn on the interface
LEAF1(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF1(config-if)# ip address 20.1.1.1/24	Configure IP address
LEAF1(config-if)#fabric forwarding mode anycast-gateway	Enable distributed anycast gateway
LEAF1(config-if)# interface Vlan300	Enter interface vlan
LEAF1(config-if)# no shutdown	Turn on the interface
LEAF1(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF1(config-if)# ip forward	Forward to vrf
LEAF1(config-if)# interface nve1	Enter interface vne
LEAF1(config-if-nve)# no shutdown	Turn on the interface
LEAF1(config-if-nve)#host-reachability protocol bgp	Set host reachability protocol bgp
LEAF1(config-if-nve)#source-interface loopback1	Set source interface
LEAF1(config-if-nve)# member vni 100	Associate L2 vni with nve
LEAF1(config-if-nve-vni)# ingress-replication protocol bgp	Enable ingress replication
LEAF1(config-if-nve)# member vni 200	Associate L2 vni with nve
LEAF1(config-if-nve-vni)# ingress-replication protocol bgp	Enable ingress replication
LEAF1(config-if-nve)#member vni 300 associate-vrf	Add L3 vni
LEAF1(config-if-nve-vni)# interface Ethernet1/1	Enter interface Ethernet1/1
LEAF1 (config-if)# no switchport	Change into routed port

LEAF1(config-if)# ip address 12.1.1.2/30	Configure IP
LEAF1(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
LEAF1(config-if)# no shutdown	Turn on the interface
LEAF1(config-if)# interface Ethernet1/6	Enter interface Ethernet1/6
LEAF1(config-if)# switchport access vlan 100	Join vlan100
LEAF1(config-if)# interface Ethernet1/7	Enter interface Ethernet1/7
LEAF1(config-if)# switchport access vlan 200	Join vlan100
LEAF1(config-if)# interface loopback1	Create loopback port
LEAF1(config-if)# ip address 3.3.3.3/32	Configure IP address
LEAF1(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
LEAF1(config-if)# router bgp 65101	Create BGP 65101 and enter routing configuration mode
LEAF1(config-router)# router-id 3.3.3.3	Configure router ID
LEAF1(config-router)# template peer LEAF1	iBGP peer template
LEAF1(config-router-neighbor)# remote-as 65101	Neighbor AS
LEAF1(config-router-neighbor)# update-source loopback1	Update source port
LEAF1(config-router-neighbor)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
LEAF1(config-router-neighbor-af)# send-community	Send community name in address family
LEAF1(config-router-neighbor-af)# send-community extended	Send community extended name in address family
LEAF1(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
LEAF1(config-router-neighbor)# address-family l2vpn evpn	Enter 12vpn evpn address family configuration mode
LEAF1(config-router-neighbor-af)# send-community	Send community name in address family
LEAF1(config-router-neighbor-af)# send-community extended	Send community extended name in address family
LEAF1(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
LEAF1(config-router-neighbor)#exit	Go back to routing configuration

	mode
LEAF1(config-router)# neighbor 1.1.1.1	Create IGBP neighbor
LEAF1(config-router-neighbor)# inherit peer LEAF1	Establish neighbor with peer template
LEAF1(config-router)# evpn	Enter EVPN configuration mode
LEAF1(config-evpn)# vni 100 l2	Create L2 VNI
LEAF1(config-evpn-evi)# rd 100:100	Configure RD
LEAF1(config-evpn-evi)# route-target import 100:100	Configure RT
LEAF1(config-evpn-evi)# route-target export 100:100	Configure RT
LEAF1(config-evpn-evi)#exit	Go back to EVPN configuration mode
LEAF1(config-evpn)# vni 200 l2	Create L2 VNI
LEAF1(config-evpn-evi)# rd 200:200	Configure RD
LEAF1(config-evpn-evi)# route-target import 200:200	Configure RT
LEAF1(config-evpn-evi)# route-target export 200:200	Configure RT

17.2.5 Leaf2 Configuration

LEAF2# configure terminal	Enter global configuration mode
LEAF2(config)# nv overlay evpn	Enable EVPN control plane for VXLAN
LEAF2(config)# feature bgp	Enable bgp
LEAF2(config)# feature ospf	Enable ospf
LEAF2(config)# feature interface-vlan	Enable interface vlan
LEAF2(config)# feature vn-segment-vlan-based	Enable VLAN-based VXLAN
LEAF2(config)# feature nv overlay	Enable vxlan
LEAF2(config)# router ospf 1	Enable OSPF protocol
LEAF2(config)# vlan 100,200,300	Create VLAN
LEAF2(config-vlan)# exit	Go back to global configuration mode
LEAF2(config)# vlan 100	Enter VLAN 100
LEAF2(config-vlan)# vn-segment 100	Create VLAN-VNI mapping
LEAF2(config-vlan)# exit	Go back to global configuration mode
LEAF2(config)# vlan 200	Enter VLAN 200
LEAF2(config-vlan)# vn-segment 200	Create VLAN-VNI mapping
LEAF2(config-vlan)# exit	Go back to global configuration

	mode
LEAF2(config)# vlan 300	Enter VLAN 300
LEAF2(config-vlan)# vn-segment 300	Create VLAN-VNI mapping
LEAF2(config)#vrf context evpn-tenant-1	Create vrf
LEAF2(config-vrf)# vni 300	Create L3 VNI
LEAF2(config-vrf)# rd 1:300	Configure RD
LEAF2(config-vrf)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
LEAF2(config-vrf-af-ipv4)#route-target import 300:300	Configure RT
LEAF2(config-vrf-af-ipv4)#route-target export 300:300	Configure RT
LEAF2(config-vrf-af-ipv4)# interface Vlan100	Enter interface vlan
LEAF2(config-if)# no shutdown	Turn on the interface
LEAF2(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF2(config-if)# ip address 10.1.1.1/24	Configure IP address
LEAF2(config-if)#fabric forwarding mode anycast-gateway	Enable distributed anycast gateway
LEAF2(config-if)# interface Vlan200	Enter interface vlan
LEAF2(config-if)# no shutdown	Turn on the interface
LEAF2(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF2(config-if)# ip address 20.1.1.1/24	Configure IP address
LEAF2(config-if)#fabric forwarding mode anycast-gateway	Enable distributed anycast gateway
LEAF2(config-if)# interface Vlan300	Enter interface vlan
LEAF2(config-if)# no shutdown	Turn on the interface
LEAF2(config-if)# vrf member evpn-tenant-1	Join vrf
LEAF2(config-if)# ip forward	Forward to vrf
LEAF2(config-if)# interface nve1	Enter interface vne
LEAF2(config-if-nve)# no shutdown	Turn on the interface
LEAF2(config-if-nve)#host-reachability protocol bgp	Set host reachability protocol bgp
LEAF2(config-if-nve)#source-interface loopback1	Set source interface
LEAF2(config-if-nve)# member vni 100	Associate L2 vni with nve
LEAF2(config-if-nve-vni)# ingress-replication protocol bgp	Enable ingress replication
LEAF2(config-if-nve)# member vni 200	Associate L2 vni with nve
LEAF2(config-if-nve-vni)# ingress-replication protocol	Enable ingress replication

bgp	
LEAF2(config-if-nve)#member vni 300 associate-vrf	Add L3 vni
LEAF2(config-if-nve-vni)# interface Ethernet1/1	Enter interface Ethernet1/1
LEAF2 (config-if)# no switchport	Change into routed port
LEAF2(config-if)# ip address 13.1.1.2/30	Configure IP
LEAF2(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on interface
LEAF2(config-if)# no shutdown	Turn on the interface
LEAF2(config-if)# interface Ethernet1/6	Enter interface Ethernet1/6
LEAF2(config-if)# switchport access vlan 100	Join vlan100
LEAF2(config-if)# interface Ethernet1/7	Enter interface Ethernet1/7
LEAF2(config-if)# switchport access vlan 200	Join vlan200
LEAF2(config-if)# interface loopback1	Create loopback port
LEAF2(config-if)# ip address 4.4.4.4/32	Configure IP address
LEAF2(config-if)# ip router ospf 1 area 0.0.0.0	Enable ospf protocol on the interface
LEAF2(config-if)# router bgp 65101	Enter BGP 65101 and enter routing configuration mode
LEAF2(config-router)# router-id 4.4.4.4	Configure router ID
LEAF2(config-router)# template peer LEAF2	iBGP peer template
LEAF2(config-router-neighbor)# remote-as 65101	Neighbor AS
LEAF2(config-router-neighbor)# update-source loopback1	Update source port
LEAF2(config-router-neighbor)# address-family ipv4 unicast	Enter ipv4 unicast address family configuration mode
LEAF2(config-router-neighbor-af)# send-community	Send community name in address family
LEAF2(config-router-neighbor-af)# send-community extended	Send community extended name in address family
LEAF2(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
LEAF2(config-router-neighbor)# address-family l2vpn evpn	Enter 12vpn evpn address family configuration mode
LEAF2(config-router-neighbor-af)# send-community	Send community name in address family
LEAF2(config-router-neighbor-af)# send-community	Send community extended name in

extended	address family
LEAF2(config-router-neighbor-af)#exit	Go back to neighbor configuration mode
LEAF2(config-router-neighbor)#exit	Go back to routing configuration mode
LEAF2(config-router)# neighbor 1.1.1.1	Create IGBP neighbor
LEAF2(config-router-neighbor)# inherit peer LEAF2	Establish neighbor with peer template
LEAF2(config-router)# evpn	Enter EVPN configuration mode
LEAF2(config-evpn)# vni 100 l2	Create L2 VNI
LEAF2(config-evpn-evi)# rd 100:100	Configure RD
LEAF2(config-evpn-evi)# route-target import 100:100	Configure RT
LEAF2(config-evpn-evi)# route-target export 100:100	Configure RT
LEAF2(config-evpn-evi)#exit	Go back to EVPN configuration mode
LEAF2(config-evpn)# vni 200 l2	Create L2 VNI
LEAF2(config-evpn-evi)# rd 200:200	Configure RD
LEAF2(config-evpn-evi)# route-target import 200:200	Configure RT
LEAF2(config-evpn-evi)# route-target export 200:200	Configure RT

17.2.6 Leaf3 Configuration

LEAF3# configure terminal	Enter global configuration mode
LEAF3(config)# ip vrf evpn-tenant-1	Create vrf
LEAF3(config-vrf)# vni 300 l3	Create L3 VNI
LEAF3(config-vrf)# rd 1:300	Configure L3 VNI RD
LEAF3(config-vrf)#route-target both 300:300	Configure L3 VNI RT
LEAF3(config-vrf)# exit	Go back to global configuration mode
LEAF3 (config)# vlan database	Enter VLAN configuration mode.
LEAF3 (config-vlan)# vlan 100,200,300	Create VLAN
LEAF3(config-vlan)# vlan 100 overlay enable	Enable vlan overlay function
LEAF3(config-vlan)# vlan 200 overlay enable	Enable vlan overlay function
LEAF3(config-vlan)# vlan 300 overlay enable	Enable vlan overlay function
LEAF3(config-vlan)# exit	Go back to global configuration mode

LEAF3(config)# overlay gateway enable	Enable overlay gateway enhance function
LEAF3(config)# overlay	Enter overlay configuration mode.
LEAF3(config-overlay)# source 7.7.7.7	Configure source vtep address of vxlan
LEAF3(config-overlay)# vtep reachability protocol bgp	Enable dynamic VxLAN tunnel construction function
LEAF3(config-overlay)# vlan 100 vni 100	Configure vlan-vni mapping
LEAF3(config-overlay)# vlan 200 vni 200	Configure vlan-vni mapping
LEAF3(config-overlay)# vlan 300 vni 300	Configure vlan-vni mapping
LEAF3(config)# evpn	Enter EVPN configuration mode
LEAF3(config-evpn)# vni 100	Create L2 VNI
LEAF3(config-evpn-evi)# rd 100:100	Configure L2 VNI RD
LEAF3(config-evpn-evi)# route-target import 100:100	Configure L2 VNI RT
LEAF3(config-evpn-evi)# route-target export 100:100	Configure L2 VNI RT
LEAF3(config-evpn-evi)#exit	Go back to EVPN configuration mode
LEAF3(config-evpn)# vni 200	Create L2 VNI
LEAF3(config-evpn-evi)# rd 200:200	Configure L2 VNI RD
LEAF3(config-evpn-evi)# route-target import 200:200	Configure L2 VNI RT
LEAF3(config-evpn-evi)# route-target export 200:200	Configure L2 VNI RT
LEAF3(config-evpn-evi)#exit	Go back to EVPN configuration mode
LEAF3(config-evpn)# exit	Go back to global configuration mode
LEAF3(config)# interface eth-0-48	Enter interface eth-0-48 configuration
LEAF3 (config-if)# no switchport	Change into routed port
LEAF3(config-if)# overlay uplink enable	Configure IP address
LEAF3(config-if)# ip address 16.1.1.2/24	Enable overlay uplink port
LEAF3(config-if)# exit	Go back to global configuration mode
LEAF3 (config)# interface vlan100	Enter interface vlan100
LEAF3(config-if)# ip vrf forwarding evpn-tenant-1	Add the interface under vrf forwarding
LEAF3(config-if)#overlay distributed-gateway enable	Enable distributed gateway

LEAF3(config-if)#overlay host-collect enable	Enable host-collect function
LEAF3(config-if)# ip address 10.3.1.1/31	Configure IP address of interface vlanif
LEAF3(config-if)# ip virtual-router address 10.1.1.1/24	Configure virtual IP address of interface vlanif
LEAF3(config-if)# exit	Go back to global configuration mode
LEAF3 (config)# interface vlan200	Enter interface vlan105
LEAF3(config-if)# ip vrf forwarding test	Add the interface under vrf forwarding
LEAF3(config-if)#overlay distributed-gateway enable	Enable distributed gateway
LEAF3(config-if)#overlay host-collect enable	Enable host-collect function
LEAF3(config-if)# ip address 20.3.1.1/24	Configure IP address of interface vlanif
LEAF3(config-if)# ip virtual-router address 20.1.1.1/24	Configure virtual IP address of interface vlanif
LEAF3(config-if)# exit	Go back to global configuration mode
LEAF3 (config)# interface loopback0	Create loopback port
LEAF3(config-if)# ip address 7.7.7.7/32	Configure IP address
LEAF3(config-if)# exit	Go back to global configuration mode
LEAF3(config)#ip virtual-router mac 0001.0001.0001	Configure virtual mac
LEAF3(config-if)# router ospf 1	Enable OSPF protocol
LEAF3(config-router)# network 7.7.7.7 0.0.0.0 area 0	Declare network segment
LEAF3(config-router)# network 16.1.1.0 0.0.0.3 area 0	Declare network segment
LEAF3(config-if)# router bgp 65101	Create BGP 65101 and enter routing configuration mode
LEAF3(config-router)# neighbor 1.1.1.1 remote-as 65101	Create IGBP neighbor
LEAF3(config-router)# neighbor 1.1.1.1 update-source loopback0	Assign update source port
LEAF3(config- router)# address-family l2vpn evpn	Enter 12vpn evpn address family configuration mode
LEAF3(config- router-af)# neighbor 1.1.1.1 activate	Activate exchanging routing information with neighbor

LEAF3(config- router-af)# exit	Go back to routing configuration mode
LEAF3(config-router)# address-family ipv4 vrf test	Enter IPV4 VRE address family configuration mode
LEAF3(config-router-af)# redistribute connected	Configure routing redistribution
LEAF3(config-router-af)# advertise l2vpn	Configure introducing routing redistribution into EVPN
LEAF3 (config-router-af)# end	Go back to user mode

Further Information:

Web www.naddod.com

Email For order requirements: sales@naddod.com

For technical support: tech@naddod.com

For technical support: tech@naddod.com

For customer service: support@naddod.com

For cooperation: agency@naddod.com

Disclaimer

1. We are committed to continuous product improvement and feature upgrades, and the contents contained in this manual are subject to change without notice.

2. Nothing herein should be construed as constituting an additional warranty.

3. NADDOD assumes no responsibility for the use or reliability of equipment or software not provided by NADDOD.

NADDOD - Explore the Digital Future of Intelligence

HPC, Networking, Data Center, ISP Solutions