PLANET
Networking & Communication

Configuration Guide

WGSW-50040

50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at whose own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the power cable to disconnect the device from the power circuit.

Without removing power cable, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

Revision

PLANET 50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch User's Manual
FOR MODEL: WGSW-50040
REVISION: 1.0 (AUGUST.2010)
Part No: EM-WGSW-50040 (2081-A93200-000)

Content

Chapter 1 INTRODUTION

The PLANET WGSW-50040 is 50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 100Gbps. Terms of "**Managed Switch**" means the Switches mentioned titled in the cover page of this User's manual.

1.1 Packet Contents

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items: Check the contents of your package for following parts:

☑ **WGSW-50040 Switch**	X1
☑ **User's Manual**	X1
☑ **Quick Installation Guide**	X1
☑ **Power Cord**	X1
☑ **RJ-45-to-DB9 Console Cable**	X1
☑ **SFP Dust Caps**	X4
☑ **Rubber Fee**	X4
☑ **Two Rack-mounting Brackets with Attachment Screws**	X1

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

Abundant IPv6 Support

The WGSW-50040 provides **IPv6 management** and enterprise level secure features such as **SSH, ACL, QoS** and **RADIUS** authentication besides the IPv4 protocol supported. Supporting IPv6 management features and also backward compatible with IPv4, the WGSW-50040 helps the enterprises to step in the IPv6 era with the lowest investment but not need to replace the network facilities while the ISP construct the IPv6 FTTx edge network.

High Performance

The WGSW-50040 provides 50 10/100/1000Mbps Gigabit Ethernet ports with 4 shared Gigabit SFP slots. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 100Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The WGSW-50040 can be programmed for basic Switch management functions such as Port speed configuration, Port aggregation, VLAN, Spanning Tree protocol, QoS, bandwidth control and IGMP Snooping. The WGSW-50040 provides 802.1Q Tagged VLAN, Q-in-Q, voice VLAN and GVRP protocol. The VLAN groups allowed on the WGSW-50040 will be maximally up to 256. By supporting port aggregation, the WGSW-50040 allows the operation of a high-speed trunk combining multiple ports. It enables up to 8 groups of maximum 8-ports for trunking.

Excellent Traffic Control

PLANET WGSW-50040 is loaded with powerful traffic management and QoS features to enhance services offered by telecoms. The functionality includes QoS features such as wire-speed Layer 4 traffic classifiers and bandwidth limiting that are particular useful for multi-tenant unit, multi business unit, Telco, or Network Service Provide applications. It also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance at VoIP and Video conferencing transmission.

Powerful Security

The WGSW-50040 supports ACL policies comprehensively. The traffic can be classified by source/destination IP addresses, source/destination MAC addresses, IP protocols, TCP/UDP, IP precedence, time ranges and ToS. Moreover, various policies can be conducted to forward the traffic. The WGSW-50040 also provides IEEE802.1x port based access authentication, which can be deployed with RADIUS, to ensure the port level security and block illegal users.

Efficient Management

The WGSW-50040 supports IP Stacking function that helps network managers to easily configure up to 24 switches in the same series via one single IP address instead of connecting and setting each unit one by one. For efficient management, the WGSW-50040 Managed Ethernet Switch is equipped with console, WEB and SNMP management interfaces. With its built-in Web-based management interface, the PLANET WGSW-50040 offers an easy-to-use, platform-independent management and configuration facility. The WGSW-50040 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, WGSW-50040 can be accessed via Telnet and the console port. Moreover, the WGSW-50040 offers secure remote management by supporting SSH connection which encrypts the packet content at each session.

Flexibility and Extension solution

The four mini-GBIC slots built in the WGSW-50040 are compatible with 1000Base-SX/LX and WDM SFP (Small Form Factor Pluggable) fiber-optic modules. The distance can be extended from 550 meters (Multi-Mode fiber) up to above 10/20/30/40/50/70/120 kilometers (Single-Mode fiber or WDM fiber). It is well suited for applications within the enterprise data centers and distributions.

1.3 Product Features

- **Physical Port**
  - 50-Port 10/100/1000Base-T Gigabit Ethernet RJ-45
  - 4 mini-GBIC/SFP slots, shared with Port-45 to Port-48
  - RJ-45 to DB9 console interface for Switch basic management and setup

- **IP Stacking**
  - Connects with stack member via both Gigabit TP/SFP interface
  - Single IP address management, supports up to 24 units stacking together
  - Stacking architecture supports Chain and Ring mode

- **Layer 2 Features**
  - Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
  - Supports Auto-negotiation and Half-Duplex / Full-Duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports.
  - Supports 1000Base-SX/LX for all SFP interfaces
  - Auto-MDI/MDI-X detection on each RJ-45 port
  - Prevents packet loss Flow Control:
    - IEEE 802.3x PAUSE Frame flow control for Full-Duplex mode
    - Back-Pressure Flow Control in Half-Duplex mode
  - High performance Store and Forward architecture, broadcast storm control, port loopback detect
  - 8CKC MAC address table, automatic source address learning and ageing
  - Support VLAN
    - IEEE 802.1Q Tag-based VLAN
    - GVRP for dynamic VLAN Management
    - Up to 4K VLANs groups, out of 4041 VLAN IDs
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN Edge (PVE) supported
    - GVRP protocol for Management VLAN
  - Support Link Aggregation
    - Maximum 8 trunk groups, up to 8 ports per trunk group
    - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
    - Cisco ether-channel (Static Trunk)
  - Spanning Tree Protocol
    - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
    - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
    - MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)
    - Supports BPDU & port guard
  - Port Mirroring to monitor the incoming or outgoing traffic on a particular port (many to many)
  - Provides Port Mirror (many-to-1)

- **Quality of Service**
  - 8 priority queues on all switch ports
  - Supports for strict priority and Weighted Round Robin (WRR) CoS policies
  - Traffic classification:
    - IEEE 802.1p CoS / ToS
    - IPv4 / IPv6 DSCP
    - Port-Based QoS
  - Strict priority and Weighted Round Robin (WRR) CoS policies

- **Multicast**
  - Support IGMP Snooping v1,v2 and v3, MLD v1 and v2 snooping
  - Querier mode support

- **Security**
  - IEEE 802.1x Port-Based network access authentication
  - MAC-Based network access authentication
  - Build-in RADIUS client to co-operate with the RADIUS servers for IPv4 and IPv6
  - TACACS+ login users access authentication
  - IP-Based Access Control List (ACL)
  - MAC-Based Access Control List
  - Supports DHCP Snooping
  - Supports ARP Inspection

- **Management**
  - Switch Management Interface
    - Console / Telnet Command Line Interface
    - Web switch management
    - SNMP v1, v2c, and v3 switch management
    - SSH secure access
  - BOOTP and DHCP for IP address assignment
  - Support DHCP relay function
  - Firmware upload / download via TFTP or HTTP protocol for IPv4 and IPv6
  - SNTP (Simple Network Time Protocol) for IPv4 and IPv6
  - User Privilege levels control
  - Syslog server for IPv4 and IPv6
  - Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events)
  - Supports Ping, Trace route function for IPv4 and IPv6
  - Management IP for IPv4 and IPv6

1.4 Product Specification

Product	**WGSW-50040** 50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
Hardware Specification	
Copper Ports	50 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports
SFP / mini-GBIC Slots	4 1000Base-SX/LX SFP interfaces, shared with Port-45 to Port-48
Switch Architecture	Store-and-Forward
Switch Fabric	100Gbps / non-blocking
Switch Throughput	74.4Mpps
Address Table	8K MAC address table with Auto learning function
Share Data Buffer	0.5Mbytes
VLAN Table	4K
ACL Table	1K
Port Queues	8
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex
Jumbo Frame	9K
LED	System: PWR, SYS Ports: TP Port:10/100/1000 Link/Act SFP Slot: On/Off
Dimension (W x D x H)	440 x 230 x 44 mm, 1U height
Weight	3215g
Power Consumption	80 Watts / 272.8 BTU (Maximum)
Power Requirement	AC 100~240V, 50/60Hz
Management Function	
System Configuration	Console, Telnet, SSH, Web Browser, SNMPv1, v2c and v3
Management	Supports the unite for IPv4 / IPv6 HTTP Supports the user IP security inspection for IPv4 / IPv6 SNMP Supports MIB and TRAP Supports IPv4 / IPv6 FTP/TFTP Supports IPv4 / IPv6 NTP Supports RMOM 1, 2, 3, 9 four group Supports the RADIUS authentication for IPv4 / IPv6 telnet user name and password Supports IPv4 / IPv6 SSH

	The right configuration for users to adopt radius server's shell management Supports CLI, Console (RS-232), Telnet Supports SNMPv1 / v2c / v3 Supports Security IP safety net management function：avoid unlawful landing at nonrestrictive area Support Syslog server for IPv4 and IPv6 Supports TACACS+
Layer2 Function	
Port Configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable/enable. Bandwidth control on each port Port Loopback detect
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status.
VLAN	802.1Q Tagged Based VLAN, up to 4K VLAN groups Q-in-Q GVRP for VLAN Management Private VLAN Edge (PVE) supported
Bandwidth Control	TX / RX / Both
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 8 groups of 8-Port trunk
QoS	8 priority queues on all switch ports Supports for strict priority and weighted round robin (WRR) CoS policies Traffic classification: - IEEE 802.1p CoS / ToS - IPv4 / IPv6 DSCP - Port-Based QoS Strict priority and Weighted Round Robin (WRR) CoS policies
IGMP Snooping	IGMP (v1 / v2) Snooping, IGMP Querier mode
Multicast	IGMP v1/ v2 / v3 Snooping IGMP Querier mode support MLDv1 / v2, MLD v1/v2 Snooping
Access Control List	Support Standard and Expanded ACL IP-Based ACL / MAC-Based ACL Time-Based ACL Up to 512 entries
Security	Support MAC + port binding IPv4 / IPv6 + MAC + port binding

	IPv4 / IPv6 + port binding Support MAC filter ARP Scanning Prevention
Authentication	IEEE 802.1x Port-Based network access control AAA Authentication: TACACS+ and IPv4 / IPv6 over RADIUS
SNMP MIBs	RFC-1213 MIB-II RFC-1215 Internet Engineering Task Force RFC-1271 RMON RFC-1354 IP-Forwarding MIB RFC-1493 Bridge MIB RFC-1643 Ether-like MIB RFC -1907 SNMP v2 RFC-2011 IP/ICMP MIB RFC-2012 TCP MIB RFC-2013 UDP MIB RFC-2096 IP forward MIB RFC-2233 if MIB RFC-2452 TCP6 MIB RFC-2454 UDP6 MIB RFC-2465 IPv6 MIB RFC-2466 ICMP6 MIB RFC-2573 SnmpV3 notify RFC-2574 SNMPV3 vacm RFC-2674 Bridge MIB Extensions (IEEE802.1Q MIB) RFC-2674 Bridge MIB Extensions (IEEE802.1P MIB)
Standard Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1s Multiple spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control

Chapter 2 INSTALLATION

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed Switch, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. Figure 2-1 shows the front panel of the Managed Switch.

WGSW-50040 Front Panel

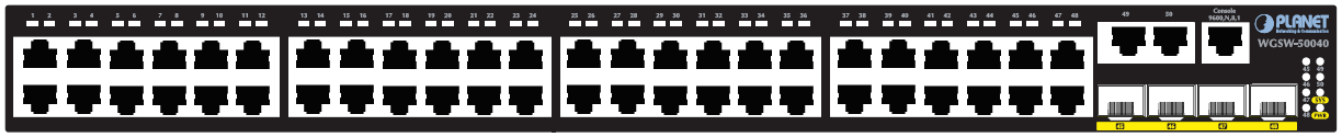


Figure 2-1 WGSW-50040 front panel

■ **Gigabit TP interface**

10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

■ **Gigabit SFP slots**

1000Base-SX/LX mini-GBIC slot, SFP (Small Form Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber), up to 10/20/30/40/50/70/120 kilometers (Single-mode fiber).

■ **Console Port**

The console port is a RJ-45 type, RS-232 male seria port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information includes IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 cable in the package and connect to the console port on the device. After the connection, users an run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the statup screen of the device.

2.1.2 LED Indications

The front panel LEDs indicates instant status of port links, data activity, system operation, Stack status and system power, helps monitor and troubleshoot when needed.

WGSW-50040 LED indication

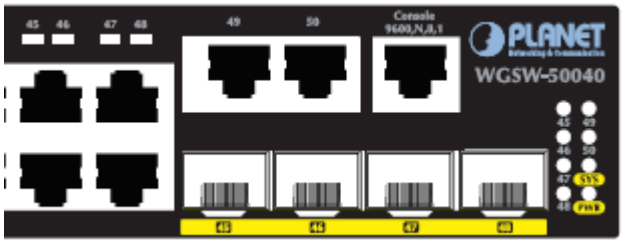


Figure 2-2 WGSW-50040 LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch has power.
	Off	Power is off.
SYS	**Green**	**Lights** to indicate the system diagnoses is completed.
		Blink to indicate boot is enable.
	Yellow	**Lights** to indicate the system diagnoses is under way.
		Blink to indicate the system diagnoses is malfunctioning.

■ **10/100/1000Base-T interfaces**

LED	Color	Function
LNK/ACT	**Green**	**Lights** to indicate the link through that port is successfully established with speed **1000Mbps**.
		Blink to indicate that the switch is actively sending or receiving data over that port.
	Yellow	**Lights** to indicate the link through that port is successfully established with speed **100Mbps** or **10Mbps**.
		Blink to indicate that the switch is actively sending or receiving data over that port.
	Off	No flow go through the port.

■ **SFP interfaces**

LED	Color	Function
LNK/ACT	**Green**	**Lights** to indicate the link through that port is successfully established with speed **1000Mbps**.
	Off	No flow go through the port.

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accept input power from 100 to 240V AC, 50-60Hz. Figure 2-3 shows the rear panel of these Managed Switch.

WGSW-50040 Rear Panel

Figure 2-3 Rear panel of **WGSW-50040**

■ **AC Power Receptacle**

For compatibility with electric service in most areas of the world, the Managed Switch's power supply automatically adjusts to line power in the range 100-240VAC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptalbe on the rear panel of the Managed Switch. Plug the other end of the power cord into an electric service outlet then the power will be ready.

Power Notice:

The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

In some area, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the Switch

This section describes how to install your Managed Switch and make connections to the Managed Switch. Please read the following topics and perform the procedures in the order being presented. To install your Managed Switch on a desktop or shelf, simply complete the following steps.

2.2.1 Desktop Installation

To install the Managed Switch on desktop or shelf, please follows these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-4.

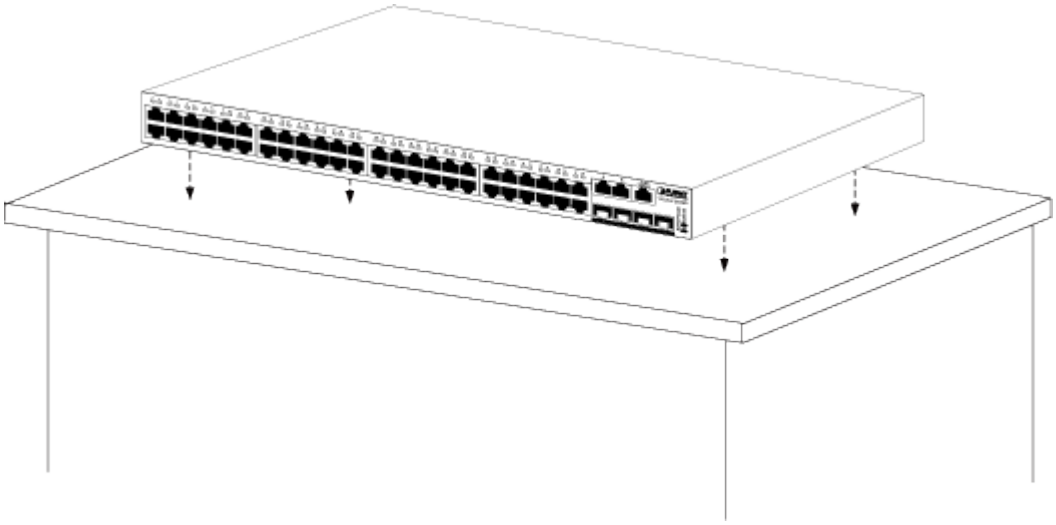


Figure 2-4 Place the Managed Switch on the desktop

Step3: Keep enough ventilation space between the Managed Switch and the surrounding objects.

Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and Specification.

Step4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch

Connect the other end of the cable to the network devices such as printer servers, workstations or routers…etc.

Note

Connection to the Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the Managed Switch.

Connect one end of the power cable to the Managed Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Managed Switch in a 19-inch standard rack, please follows the instructions described below.

Step1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package. Figure 2-5 shows how to attach brackets to one side of the Managed Switch.

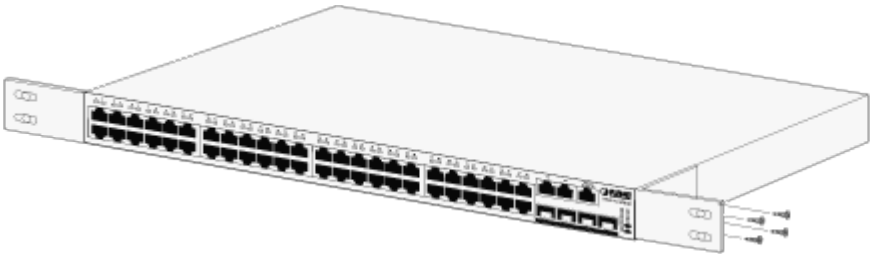


Figure 2-5 Attach brackets to the Managed Switch.

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6.

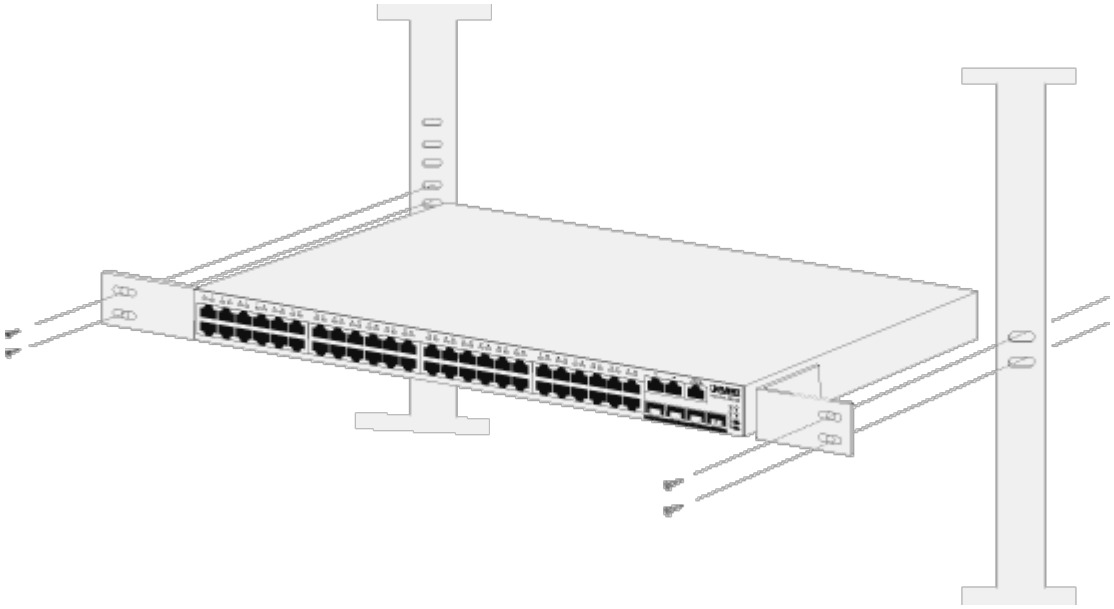


Figure 2-6 Mounting WGSW-50040 in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed Switch. As the Figure 2-7 appears.

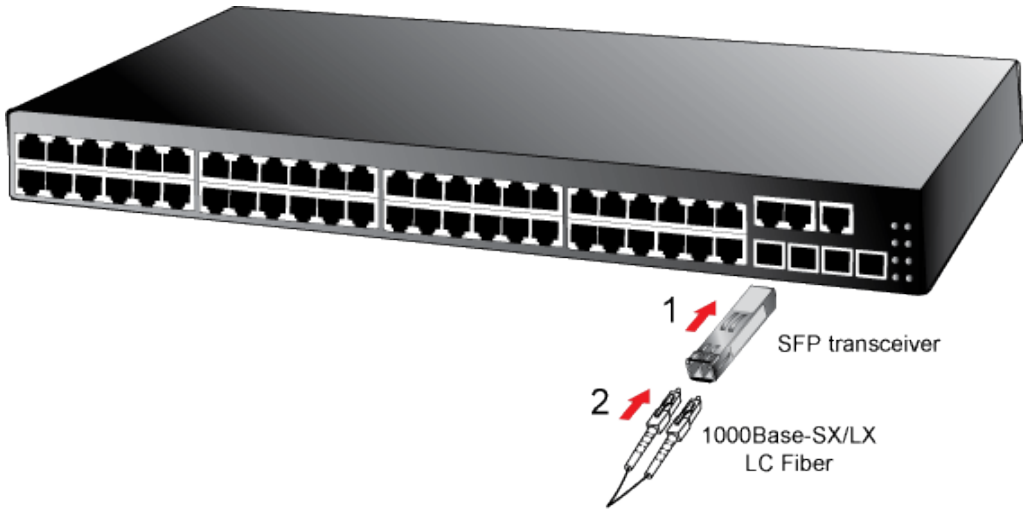


Figure 2-7 Plug-in the SFP transceiver

■ **Approved PLANET SFP Transceivers**

PLANET Managed Switch supports both Single mode and Multi-mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Gigabit SFP Transceiver modules:

■ **MGB-SX** SFP (1000BASE-SX SFP transceiver / Multi-mode / 850nm / 220m~550m)

■ **MGB-LX** SFP (1000BASE-LX SFP transceiver / Single-mode / 1310nm / 10km)

■ **MGB-L30** SFP (1000BASE-LX SFP transceiver / Single-mode / 1310nm / 30km)

■ **MGB-L50** SFP (1000BASE-LX SFP transceiver / Single-mode / 1310nm / 50km)

■ **MGB-LA10** SFP (1000BASE-LX SFP transceiver / WDM Single-mode / TX: 1310nm, RX: 1550nm/ 10km)

■ **MGB-LB10** SFP (1000BASE-LX SFP transceiver / WDM Single-mode / TX: 1550nm, RX: 1310nm / 10km)

Note

It recommends using PLANET SFPs on the Managed Switch. If you insert a SFP transceiver that is not supported, the Managed Switch will not recognize it.

Before connect the other Managed Switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable-with one side must be male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable-with one side must

be male duplex LC connector type.

■ **Connect the fiber cable**

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to “1000 Force” is needed.

■ **Remove the transceiver module**

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB module to horizontal.
4. Pull out the module gently through the handle.

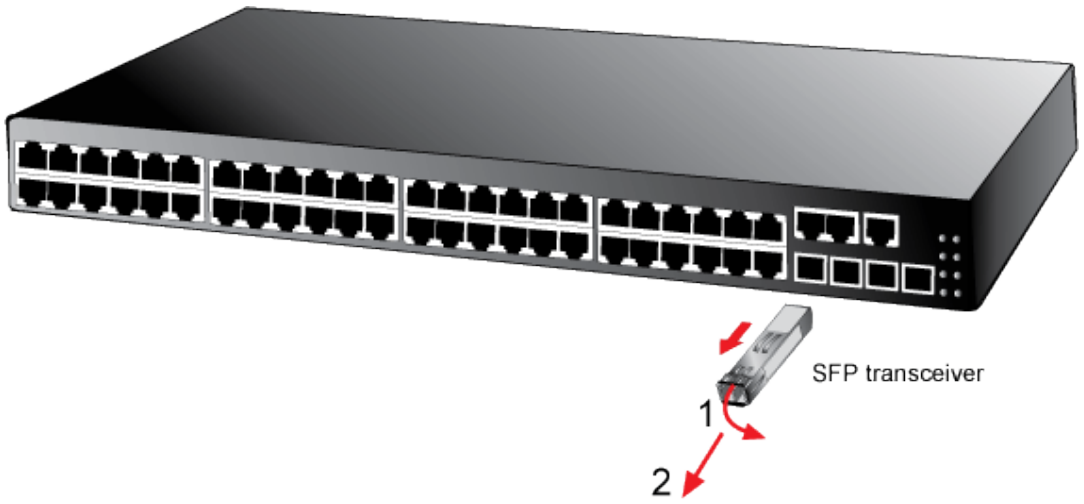


Figure 2-8 Pull out the SFP transceiver

Note

Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the Managed Switch.

Chapter 3 Switch Management

3.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. Switch provides two management options: in-band management and out-of-band management.

3.1.1 Out-Of-Band Management

Out-of-band management is the management through Console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available. For instance, the user must assign an IP address to the switch via the Console interface to be able to access the switch through Telnet.
The procedures for managing the switch via Console interface are listed below:

Step 1: Setting up the environment:

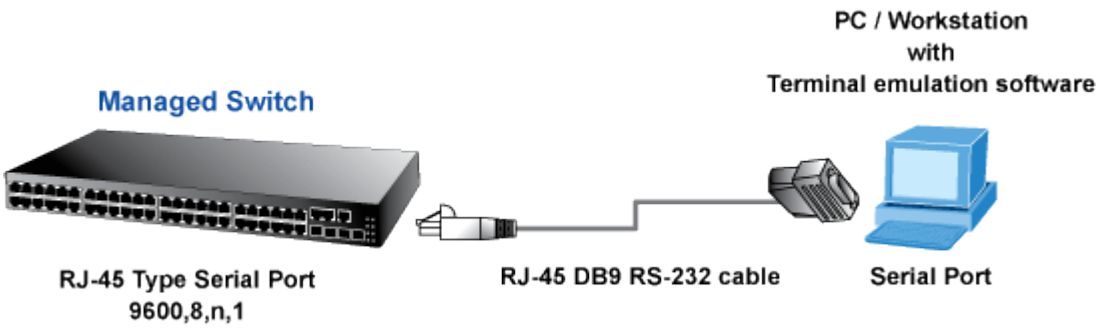


Figure 3-1 Out-of-band Management Configuration Environment

As shown in above, the serial port (RS-232) is connected to the switch with the serial cable provided. The table below lists all the devices used in the connection.

Device Name	Description
PC machine	Has functional keyboard and RS-232, with terminal emulator installed, such as HyperTerminal included in Windows 9x/NT/2000/XP.
Serial port cable	One end attach to the RS-232 serial port, the other end to the Console port.
Switch	Functional Console port required.

Step 2： **Entering the HyperTerminal**

Open the HyperTerminal included in Windows after the connection established. The example below is based on the HyperTerminal included in Windows XP.

1) Click Start menu - All Programs -Accessories -Communication - **HyperTerminal**.

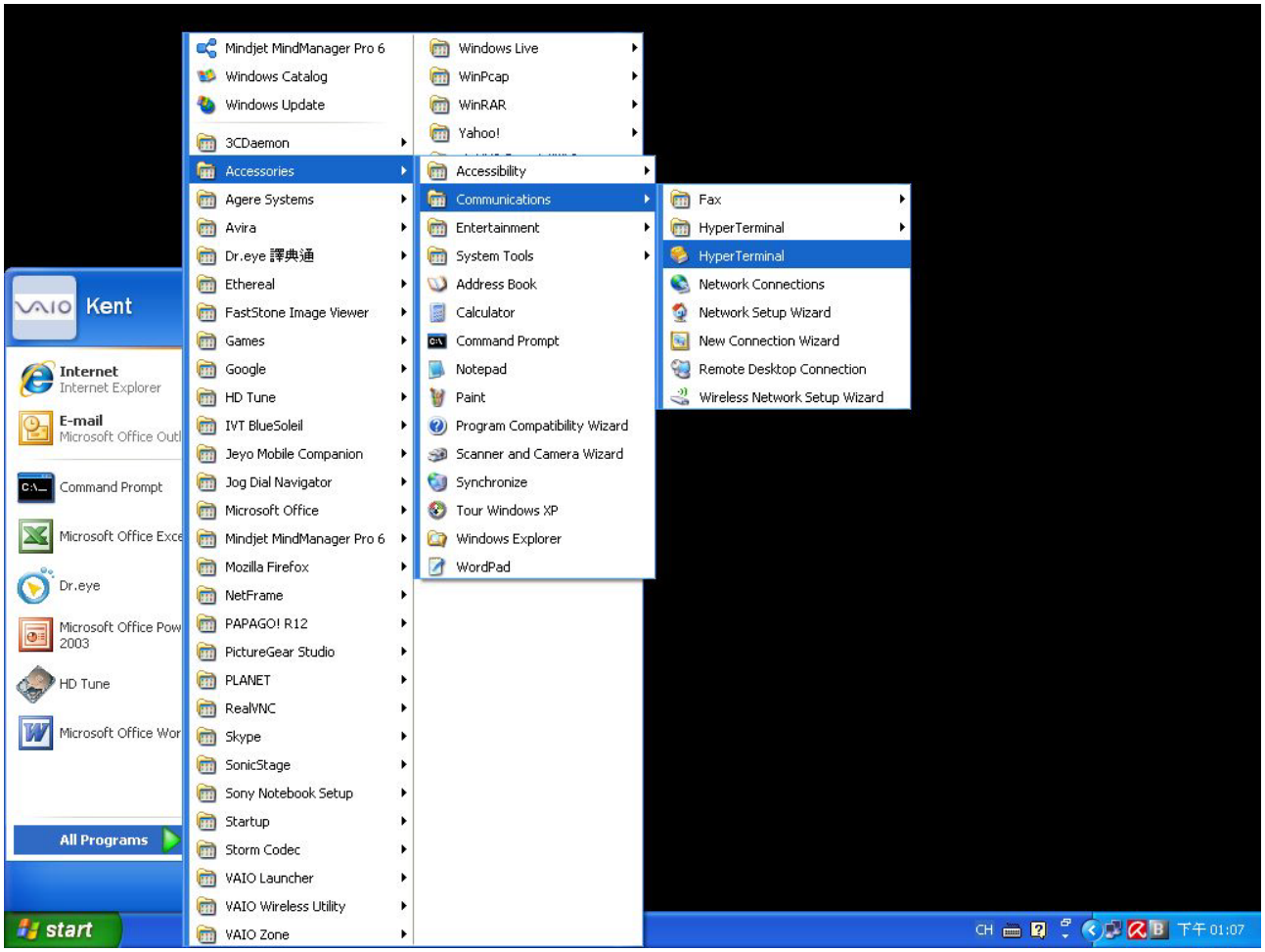


Figure 3-2 Opening Hyper Terminal

2) Type a name for opening HyperTerminal, such as “Switch”.

Figure 3-3 Opening HyperTerminal

3) In the “Connecting using” drop-list, select the RS-232 serial port used by the PC, e.g. COM1, and click “OK”.

Figure 3-4 Opening HyperTerminal

4) COM1 property appears, select “9600” for “Baud rate”, “8” for “Data bits”, “none” for “Parity checksum”, “1” for stop bit and “none” for traffic control; or, you can also click “Restore default” and click “OK”.

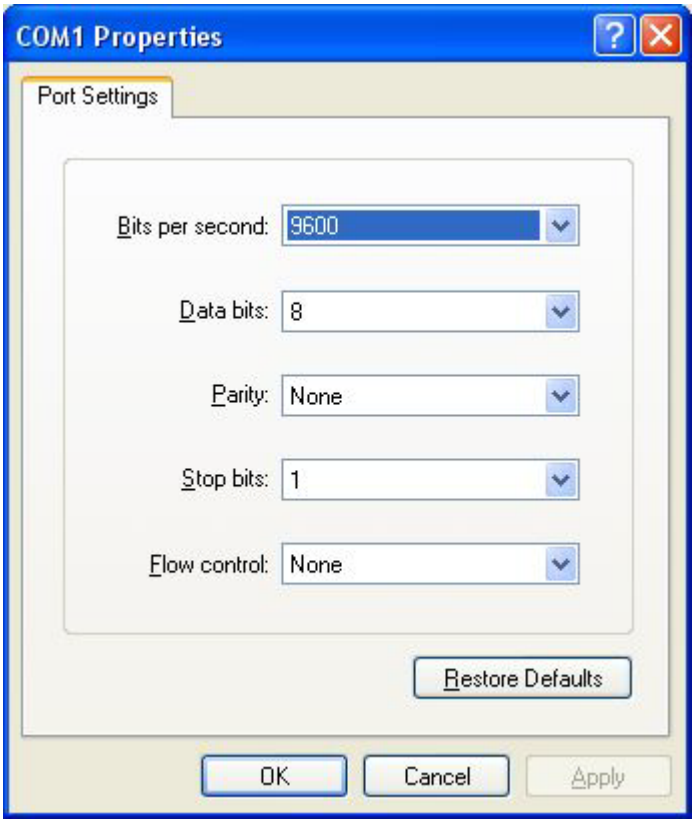


Figure 3-5 Opening HyperTerminal

Step 3: Entering switch CLI interface

Power on the switch, the following appears in the HyperTerminal windows, that is the CLI configuration mode for Switch.

```
Testing RAM...
0x077C0000 RAM OK
Loading MiniBootROM...
Attaching to file system ...

Loading nos.img ...   done.
Booting......
Starting at 0x10000...

Attaching to file system ...
……
--- Performing Power-On Self Tests (POST) ---
DRAM Test.....PASS!
PCI Device 1 Test.....PASS!
FLASH Test.....PASS!
FAN Test.....PASS!
Done All Pass.
------------------ DONE ----------------------
Current time is SUN JAN 01 00:00:00 2006
……
Switch>
```

The user can now enter commands to manage the switch. For a detailed description for the commands, please refer to the following chapters.

3.1.2 In-band Management

In-band management refers to the management by login to the switch using Telnet, or using HTTP, or using SNMP management software to configure the switch. In-band management enables management of the switch for some devices attached to the switch. In the case when in-band management fails due to switch configuration changes, out-of-band management can be used for configuring and managing the switch.

3.1.2.1 Management via Telnet

To manage the switch with Telnet, the following conditions should be met:

1) Switch has an IPv4/IPv6 address configured;
2) The host IP address (Telnet client) and the switch's VLAN interface IPv4/IPv6 address is in the same network segment;
3) If 2) is not met, Telnet client can connect to an IPv4/IPv6 address of the switch via other devices, such as a router.

The switch is Layer 3 switch that can be configured with several IPv4/IPv6 addresses. The following example assumes the shipment status of the switch where only VLAN1 exists in the system. The following describes the steps for a Telnet client to connect to the switch's VLAN1 interface by Telnet (with IPv4 address example):

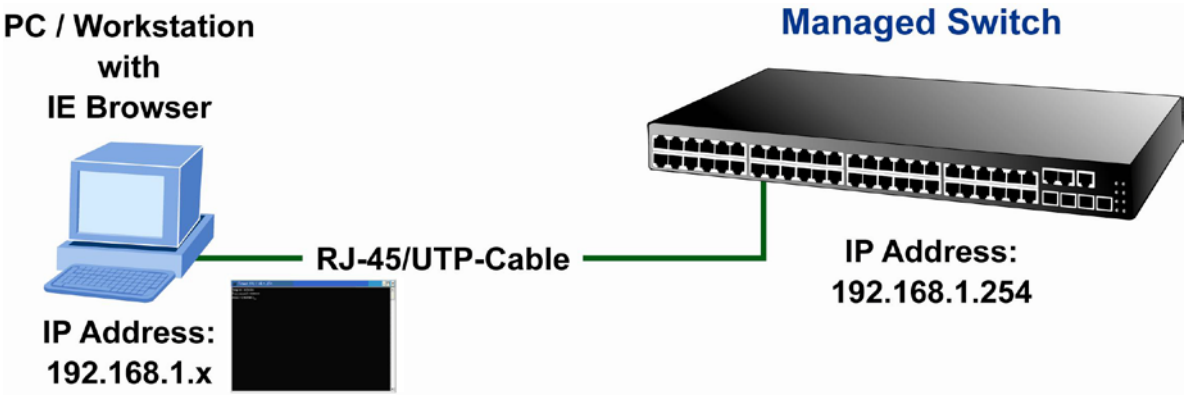


Figure 3-6 Manage the switch by Telnet

Step 1: Configure the IP addresses for the switch and start the Telnet Server function on the switch.
First is the configuration of host IP address. This should be within the same network segment as the switch VLAN1 interface IP address. Suppose the switch VLAN1 interface IP address is 10.1.128.251/24. Then, a possible host IP address is 10.1.128.252/24. Run "ping 10.1.128.251" from the host and verify the result, check for reasons if ping failed.

The IP address configuration commands for VLAN1 interface are listed below. Before in-band management, the switch must be configured with an IP address by out-of-band management (i.e. Console mode), the configuration commands are as follows (All switch configuration prompts are assumed to be "Switch" hereafter if not otherwise specified):

```
Switch>
Switch>enable
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-if-Vlan1)#no shutdown
```

To enable the Telnet Server function, users should type the CLI command telnet-server enable in the global mode as below:

```
Switch>en
Switch#config
Switch(config)# telnet-server enable
```

Step 2: Run Telnet Client program.

Run Telnet client program included in Windows with the specified Telnet target.

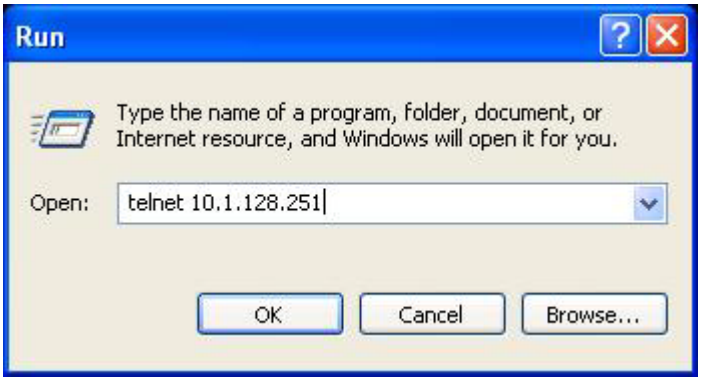


Figure 3-7 Run telnet client program included in Windows

Step 3: Login to the switch.

Login to the Telnet configuration interface. Valid login name and password are required, otherwise the switch will reject Telnet access. This is a method to protect the switch from unauthorized access. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command:

username <username> privilege <privilege> [password (0|7) <password>].

To open the local authentication style with the following command: authentication line vty login local. Privilege option must exist and just is 15. Assume an authorized user in the switch has a username of “test”, and password of “test”, the configuration procedure should like the following:

Switch>enable Switch#config Switch(config)#**username test privilege 15 password 0 test** Switch(config)#authentication line vty login local

Enter valid login name and password in the Telnet configuration interface, Telnet user will be able to enter the switch’s CLI configuration interface. The commands used in the Telnet CLI interface after login is the same as that in the Console interface.

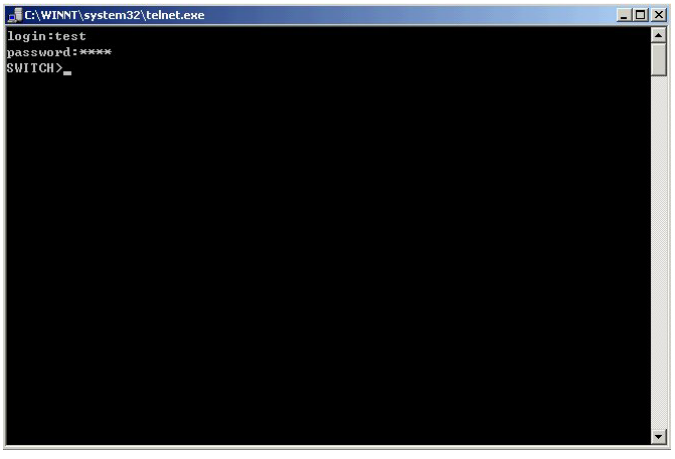


Figure 3-8 Telnet Configuration Interface

3.1.2.2 Management via HTTP

To manage the switch via HTTP, the following conditions should be met:

1) Switch has an IPv4/IPv6 address configured;

2) The host IPv4/IPv6 address (HTTP client) and the switch's VLAN interface IPv4/IPv6 address are in the same network segment;

3) If 2) is not met, HTTP client should connect to an IPv4/IPv6 address of the switch via other devices, such as a router.

Similar to management the switch via Telnet, as soon as the host succeeds to ping/ping6 an IPv4/IPv6 address of the switch and to type the right login password, it can access the switch via HTTP. The configuration list is as below:

Step 1: Configure the IP addresses for the switch and start the HTTP server function on the switch.
For configuring the IP address on the switch through out-of-band management, see the telnet management chapter.

To enable the WEB configuration, users should type the CLI command IP http server in the global mode as below:

```
Switch>enable
Switch#config
Switch(config)#ip http server
```

Step 2: Run HTTP protocol on the host.
Open the Web browser on the host and type the IP address of the switch, or run directly the HTTP protocol on the Windows. For example, the IP address of the switch is "10.1.128.251";

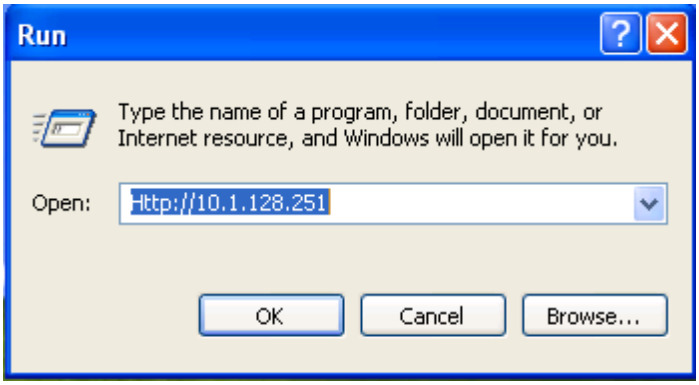


Figure 3-9 Run HTTP Protocol

When accessing a switch with IPv6 address, it is recommended to use the Firefox browser with 1.5 or later version. For example, if the IPv6 address of the switch is 3ffe:506:1:2::3. Input the IPv6 address of the switch is **http://[3ffe:506:1:2::3]** and the address should draw together with the square brackets.

Step 3: Login to the switch.

Login to the Web configuration interface. Valid login name and password are required, otherwise the switch will reject HTTP access. This is a method to protect the switch from unauthorized access. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command:

username <*username*> privilege <*privilege*> [password (0|7) <*password*>]

To open the local authentication style with the following command: **authentication line web login local.** ***Privilege*** option must exist and just is 15. Assume an authorized user in the switch has a username of "admin", and password of "admin", the configuration procedure should like the following:

```
Switch>enable
Switch#config
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#authentication line web login local
```

The Web login interface of WGSW-50040 is as below:

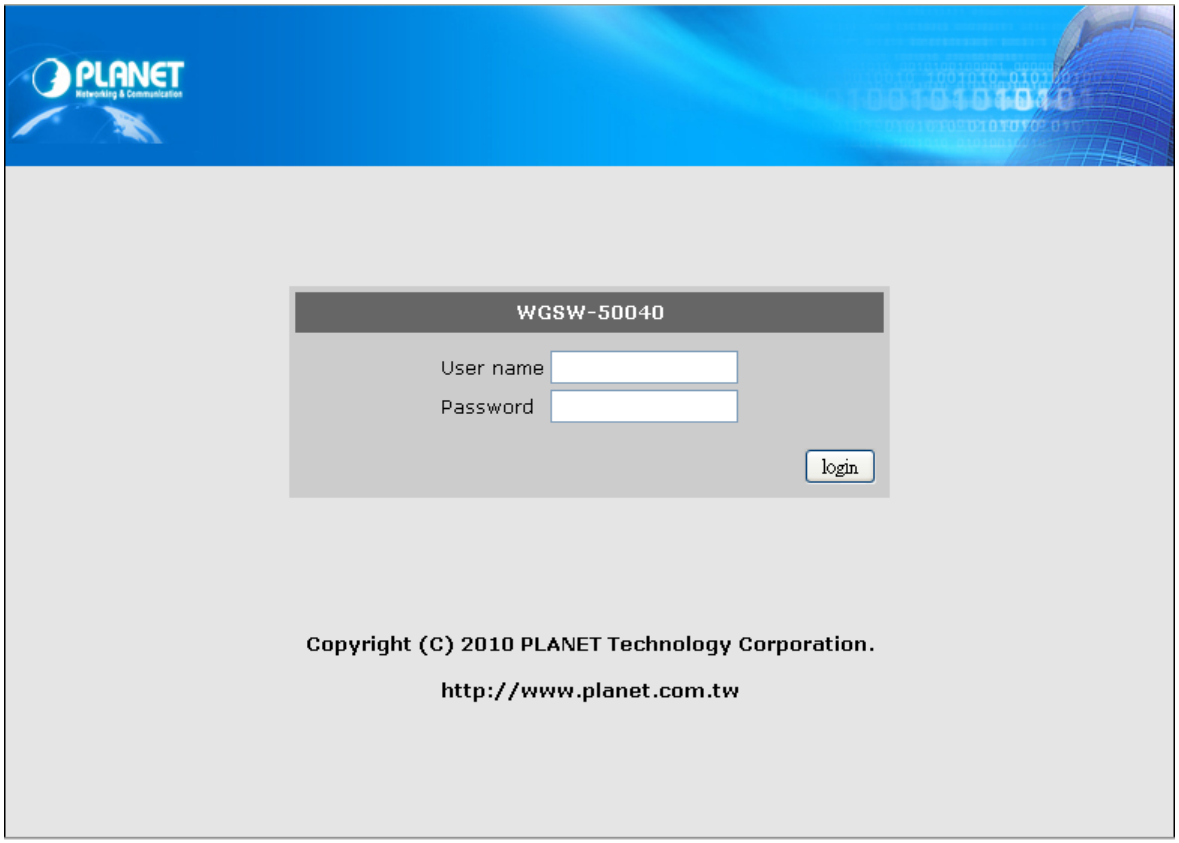


Figure 3-10 Web Login Interface

Input the right username and password, and then the main Web configuration interface is shown as below.

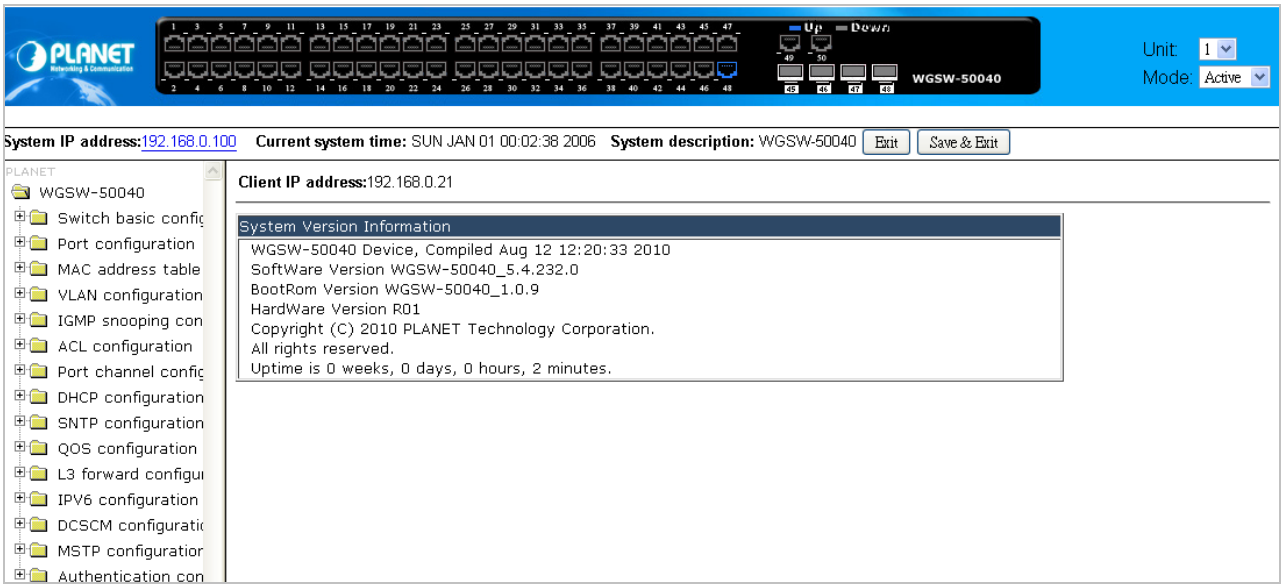


Figure 3-11 Main Web Configuration Interface

Note	When configure the switch, the name of the switch is composed with English letters.

3.1.2.3 Manage the Switch via SNMP Network Management Software

The necessities required by SNMP network management software to manage switches:

1) IP addresses are configured on the switch;
2) The IP address of the client host and that of the VLAN interface on the switch it subordinates to should be in the same segment;
3) If 2) is not met, the client should be able to reach an IP address of the switch through devices like routers;
4) SNMP should be enabled.

The host with SNMP network management software should be able to ping the IP address of the switch, so that, when running, SNMP network management software will be able to find it and implement read/write operation on it. Details about how to manage switches via SNMP network management software will not be covered in this manual, please refer to “Snmp network management software user manual”.

3.2 CLI Interface

The switch provides thress management interface for users: CLI (Command Line Interface) interface, Web interface, Snmp network management software. We will introduce the CLI interface and Web configuration interface in details, Web interface is familiar with CLI interface function and will not be covered, please refer to “Snmp network management software user manual”.

CLI interface is familiar to most users. As aforementioned, out-of-band management and Telnet login are all performed through CLI interface to manage the switch.

CLI Interface is supported by Shell program, which consists of a set of configuration commands. Those commands are categorized according to their functions in switch configuration and management. Each category represents a different configuration mode. The Shell for the switch is described below:

- Configuration Modes
- Configuration Syntax
- Shortcut keys
- Help function
- Input verification
- Fuzzy match support

3.2.1 Configuration Modes

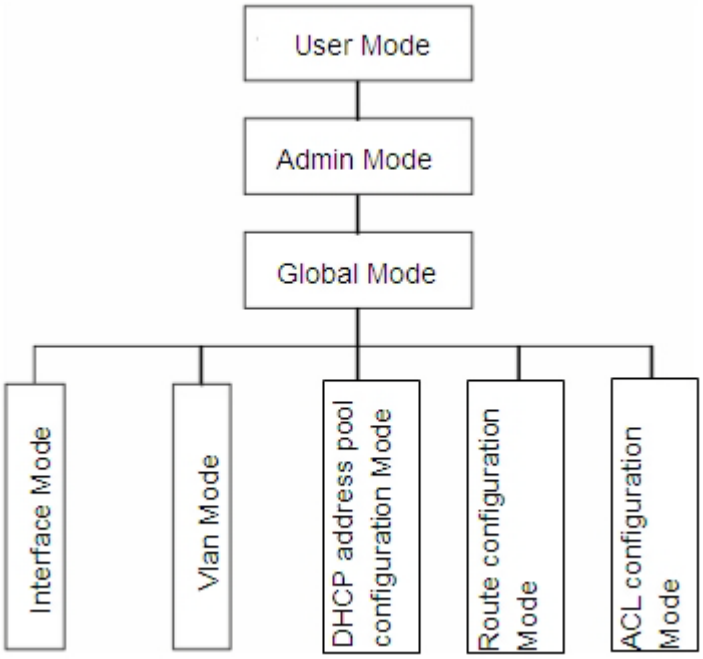


Figure 3-12 Shell Configuration Modes

3.2.1.1 User Mode

On entering the CLI interface, entering user entry system first. If as common user, it is defaulted to User Mode. The prompt shown is **"Switch>**", the symbol ">" is the prompt for User Mode. When exit command is run under Admin Mode, it will also return to the User Mode.

Under User Mode, no configuration to the switch is allowed, only clock time and version information of the switch can be queries.

3.2.1.2 Admin Mode

To Admin Mode sees the following: In user entry system, if as Admin user, it is defaulted to Admin Mode. Admin Mode prompt "**Switch#**" can be entered under the User Mode by running the enable command and entering corresponding access levels admin user password, if a password has been set. Or, when exit command is run under Global Mode, it will also return to the Admin Mode. Switch also provides a shortcut key sequence "**Ctrl+z**", this allows an easy way to exit to Admin Mode from any configuration mode (except User Mode).

Under Admin Mode, the user can query the switch configuration information, connection status and traffic statistics of all ports; and the user can further enter the Global Mode from Admin Mode to modify all configurations of the switch. For this reason, a password must be set for entering Admin mode to prevent unauthorized access and malicious modification to the switch.

3.2.1.3 Global Mode

Type the config command under Admin Mode will enter the Global Mode prompt "**Switch(config)#**". Use the exit command under other configuration modes such as Port Mode, VLAN mode will return to Global Mode.

The user can perform global configuration settings under Global Mode, such as MAC Table, Port Mirroring, VLAN creation, IGMP Snooping start and STP, etc. And the user can go further to Port Mode for configuration of all the interfaces.

- **Interface Mod**

Use the interface command under Global Mode can enter the interface mode specified. Switch provides three interface type: 1. VLAN interface; 2. Ethernet port; 3. port-channel, accordingly the three interface configuration modes.

Interface Type	Entry	Operates	Exit
VLAN Interface	Type **interface vlan <*Vlan-id*>** command under Global Mode.	Configure switch IPs, etc	Use the **exit** command to return to Global Mode.
Ethernet Port	Type **interface ethernet <interface-list>** command under Global Mode.	Configure supported duplex mode, speed, etc. of Ethernet Port.	Use the **exit** command to return to Global Mode.
port-channel	Type **interface port-channel <port-channel-number>** command under Global Mode.	Configure port-channel related settings such as duplex mode, speed, etc.	Use the **exit** command to return to Global Mode.

- **VLAN Mode**

  Using the **vlan <vlan-id>** command under Global Mode can enter the corresponding VLAN Mode. Under VLAN Mode the user can configure all member ports of the corresponding VLAN. Run the exit command to exit the VLAN Mode to Global Mode.

- **DHCP Address Pool Mode**

Type the **ip dhcp pool <name>** command under Global Mode will enter the DHCP Address Pool Mode prompt "Switch(Config-<name>-dhcp)#". DHCP address pool properties can be configured under DHCP Address Pool Mode. Run the exit command to exit the DHCP Address Pool Mode to Global Mode.

- **ACL Mode**

ACL type	Entry	Operates	Exit
Standard IP ACL Mode	**Type ip access-list standard command under Global Mode.**	Configure parameters for Standard IP ACL Mode.	Use the **exit** command to return to Global Mode.
Extended IP ACL Mode	**Type ip access-list extanded command under Global Mode.**	Configure parameters for Extended IP ACL Mode.	Use the **exit** command to return to Global Mode.

3.2.2 Configuration Syntax

Switch provides various configuration commands. Although all the commands are different, they all abide by the syntax for Switch configuration commands. The general commands format of Switch is shown below:

cmdtxt <*variable*> {enum1 | … | enumN } [option1 | … | optionN]

Conventions: **cmdtxt** in bold font indicates a command keyword; **<*variable*>** indicates a variable parameter; **{enum1 | … | enumN }** indicates a mandatory parameter that should be selected from the parameter set **enum1~enumN**; and the square bracket ([ ]) in **[option1 | … | optionN]** indicate an optional parameter. There may be combinations of "< >", "{ }" and "[ ]" in the command line, such as **[<*variable*>]**, **{enum1 <*variable*>| enum2}**, **[option1 [option2]], etc.**

Here are examples for some actual configuration commands:

- show version, no parameters required. This is a command with only a keyword and no parameter, just type in the command to run.
- vlan <vlan-id>, parameter values are required after the keyword.
- firewall {enable | disable}, user can enter firewall enable or firewall disable for this command.
- snmp-server community {ro | rw} <*string*>, the followings are possible:

  snmp-server community ro <string>

  snmp-server community rw <string>

3.2.3 Shortcut Key Support

Switch provides several shortcut keys to facilitate user configuration, such as up, down, left, right and Blank Space. If the terminal does not recognize Up and Down keys, **ctrl +p** and **ctrl +n** can be used instead.

Key(s)	Function
Back Space	Delete a character before the cursor, and the cursor moves back.
Up "↑"	Show previous command entered. Up to ten recently entered

	commands can be shown.	
Down "↓"	Show next command entered. When use the Up key to get previously entered commands, you can use the Down key to return to the next command	
Left "←"	The cursor moves one character to the left.	You can use the Left and Right key to modify an entered command.
Right "→"	The cursor moves one character to the right.	
Ctrl +p	The same as Up key "↑".	
Ctrl +n	The same as Down key "↓".	
Ctrl +b	The same as Left key "←".	
Ctrl +f	The same as Right key "→".	
Ctrl +z	Return to the Admin Mode directly from the other configuration modes (except User Mode).	
Ctrl +c	Break the ongoing command process, such as ping or other command execution.	
Tab	When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.	

3.2.4 Help Function

There are two ways in Switch for the user to access help information: the "help" command and the "?".

Access to Help	Usage and function
Help	Under any command line prompt, type in "help" and press Enter will get a brief description of the associated help system.
"?"	1· Under any command line prompt, enter "?" to get a command list of the current mode and related brief description. 2· Enter a "?" after the command keyword with a embedded space. If the position should be a parameter, a description of that parameter type, scope, etc, will be returned; if the position should be a keyword, then a set of keywords with brief description will be returned; if the output is "<cr>", then the command is complete, press Enter to run the command. 3· A "?" immediately following a string. This will display all the commands that begin with that string.

3.2.5 Input Verification

3.2.5.1 Returned Information: success

All commands entered through keyboards undergo syntax check by the Shell. Nothing will be returned if the user entered a correct command under corresponding modes and the execution is successful.

Returned Information: error

Output error message	Explanation
Unrecognized command or illegal parameter!	The entered command does not exist, or there is error in parameter scope, type or format.
Ambiguous command	At least two interpretations is possible basing on the current input.
Invalid command or parameter	The command is recognized, but no valid parameter record is found.
This command is not exist in current mode	The command is recognized, but this command can not be used under current mode.
Please configure precursor command "*" at first!	The command is recognized, but the prerequisite command has not been configured.
syntax error : missing '"' before the end of command line!	Quotation marks are not used in pairs.

3.2.6 Fuzzy Match Support

Switch shell support fuzzy match in searching command and keyword. Shell will recognize commands or keywords correctly if the entered string causes no conflict.

For example:

1) For command “show interfaces status ethernet1/1”, typing “sh in status ethernet1/1” will work.

2) However, for command “show running-config”, the system will report a “> Ambiguous command!” error if only “show r” is entered, as Shell is unable to tell whether it is “show run” or “show running-config”. Therefore, Shell will only recognize the command if “sh ru” is entered.

Chapter 4 Basic Switch Configuration

4.1 Basic Configuration

Basic switch configuration includes commands for entering and exiting the admin mode, commands for entering and exiting interface mode, for configuring and displaying the switch clock, for displaying the version information of the switch system, etc.

Command	**Explanation**
Normal User Mode/ Admin Mode	
enable **disable**	The User uses **enable** command to step into admin mode from normal user mode. The **disable** command is for exiting admin mode.
Admin Mode	
config [terminal]	Enter global mode from admin mode.
Various Modes	
exit	Exit current mode and enter previous mode, such as using this command in global mode to go back to admin mode, and back to normal user mode from admin mode.
Except User Mode/ Admin Mode	
end	Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.
Admin Mode	
clock set *<HH:MM:SS>* **[YYYY.MM.DD]**	Set system date and time.
show version	Display version information of the switch.
set default	Restore to the factory default.
write	Save current configuration parameters to Flash Memory.
reload	Hot reset the switch.

4.2 Telnet Management

4.2.1 Telnet

4.2.1.1 Introduction to Telnet

Telnet is a simple remote terminal protocol for remote login. Using Telnet, the user can login to a remote host with its IP address of hostname from his own workstation. Telnet can send the user's keystrokes to the remote host and send the remote host output to the user's screen through TCP connection. This is a transparent service, as to the user, the keyboard and monitor seems to be connected to the remote host directly.

Telnet employs the Client-Server mode, the local system is the Telnet client and the remote host is the Telnet server. Switch can be either the Telnet Server or the Telnet client.

When switch is used as the Telnet server, the user can use the Telnet client program included in Windows or the other operation systems to login to switch, as described earlier in the In-band management section. As a Telnet server, switch allows up to 5 telnet client TCP connections.

And as Telnet client, using telnet command under Admin Mode allows the user to login to the other remote hosts. Switch can only establish TCP connection to one remote host. If a connection to another remote host is desired, the current TCP connection must be dropped.

4.2.1.2 Telnet Configuration Task List

1. Configuring Telnet Server
2. Telnet to a remote host from the switch.

1. Configuration of Telnet Server

Command	Explanation
Global Mode	
telnet-server enable **no telnet-server enable**	Enable the Telnet server function in the switch: the "**no telnet-server enable**" command disables the Telnet function.
username <*user-name*> [privilege <*privilege*>] [password {0 | 7} <*password*>] **no username <*username*>**	Configure user name and password of the telnet. The **no** form command deletes the telnet user authorization.
authentication securityip <*ip-addr*> **no authentication securityip <*ip-addr*>**	Configure the secure IP address to login to the switch through Telnet: the **no** command deletes the authorized Telnet secure address.
authentication securityipv6 <*ipv6-addr*> **no authentication securityipv6 <*ipv6-addr*>**	Configure the secure IPv6 address to login to the switch through Telnet: the no command deletes the authorized Telnet secure address.

authentication ip access-class {<num-std>|<name>} **no authentication ip access-class**	Binding standard IP ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.
authentication ipv6 access-class {<num-std>|<name>} **no authentication ipv6 access-class**	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.
authentication line {console | vty | web} login {local | radius | tacacs } **no authentication line {console | vty | web} login**	Configure telnet authentication mode.
Admin Mode	
terminal monitor **terminal no monitor**	Display debug information for Telnet client login to the switch; the **no** command disables the debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
telnet {*<ip-addr>* | *<ipv6-addr>* | host *<hostname>*} [*<port>*]	Login to a remote host with the Telnet client included in the switch.

4.2.2 SSH

4.2.2.1 Introduction to SSH

SSH (Secure Shell) is a protocol which ensures a secure remote access connection to network devices. It is based on the reliable TCP/IP protocol. By conducting the mechanism such as key distribution, authentication and encryption between SSH server and SSH client, a secure connection is established. The information transferred on this connection is protected from being intercepted and decrypted. The switch meets the requirements of SSH2.0. It supports SSH2.0 client software such as SSH Secure Client and putty. Users can run the above software to manage the switch remotely.

The switch presently supports **RSA authentication**, **3DES cryptography** protocol and SSH user password authentication etc.

4.2.2.2 SSH Server Configuration Task List

SSH Server Configuration

Command	Explanation
Global Mode	
ssh-server enable **no ssh-server enable**	Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
ssh-user <*user-name*> password {0 | 7} <*password*> **no ssh-user <*user-name*>**	Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.
ssh-server timeout <*timeout*> **no ssh-server timeout**	Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.
ssh-server authentication-retires <*authentication-retires*> **no ssh-server authentication-retries**	Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.
ssh-server host-key create rsa modulus <*moduls*>	Generate the new RSA host key on the SSH server.
Admin Mode	
terminal monitor **terminal no monitor**	Display SSH debug information on the SSH client side; the "**no terminal monitor**" command stops displaying SSH debug information on the SSH client side.

4.2.2.3 Typical SSH Server Configuration

Example1:

Requirement: Enable SSH server on the switch, and run SSH2.0 client software such as Secure shell client or putty on the terminal. Log on the switch by using the username and password from the client.

Configure the IP address, add SSH user and enable SSH service on the switch. SSH2.0 client can log on the switch by using the username and password to configure the switch.

```
Switch(config)#ssh-server enable
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 100.100.100.200 255.255.255.0
```

```
Switch(Config-if-Vlan1)#exit
Switch(config)# username test privilege 15 password 0 test
```

In IPv6 networks, the terminal should run IPv6-supporing SSH client software, such as putty6. Users should make no modification to configurations on the switch except allocating an IPv6 address for the local host.

4.3 Configurate Switch IP Addresses

All Ethernet ports of switch are default to Data Link layer ports and perform layer 2 forwarding. VLAN interface represent a Layer 3 interface function which can be assigned an IP address, which is also the IP address of the switch. All VLAN interface related configuration commands can be configured under VLAN Mode. Switch provides three IP address configuration methods:

- Manual
- BOOTP
- DHCP

Manual configuration of IP address is assign an IP address manually for the switch.

In BOOTP/DHCP mode, the switch operates as a BOOTP/DHCP client, send broadcast packets of BOOTPRequest to the BOOTP/DHCP servers, and the BOOTP/DHCP servers assign the address on receiving the request. In addition, switch can act as a DHCP server, and dynamically assign network parameters such as IP addresses, gateway addresses and DNS server addresses to DHCP clients DHCP Server configuration is detailed in later chapters.

4.3.1 Switch IP Addresses Configuration Task List

1． Enable VLAN port mode
2． Manual configuration
3． BOOTP configuration
4． DHCP configuration

1. Enable VLAN port mode

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Create VLAN interface (layer 3 interface); the " **no interface vlan <*vlan-id*>** " command deletes the VLAN interface.

2. Manual configuration

Command	Explanation
VLAN Port Mode	

ip address <*ip_address*> <*mask*> [secondary] **no ip address <*ip_address*> <*mask*> [secondary]**	Configure the VLAN interface IP address; the "**no ip address <*ip_address*> <*mask*> [secondary]**" command deletes VLAN interface IP address.
ipv6 address <*ipv6-address / prefix-length*> [eui-64] **no ipv6 address <*ipv6-address / prefix-length*>**	Configure IPv6 address, including aggregation global unicast address, local site address and local link address. The **no** form command deletes IPv6 address.

3. BOOTP configuration

Command	Explanation
VLAN Port Mode	
ip bootp-client enable **no ip bootp-client enable**	Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP client function.

4. DHCP configuration

Command	Explanation
VLAN Port Mode	
ip bootp-client enable **no ip bootp-client enable**	Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip bootp-client enable**" command disables the DHCP client function.

4.4 SNMP Configuration

4.4.1 Introduction to SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol widely used in computer network management. SNMP is an evolving protocol. SNMP v1 [RFC1157] is the first version of SNMP which is adapted by vast numbers of manufacturers for its simplicity and easy implementation; SNMP v2c is an enhanced version of SNMP v1, which supports layered network management; SNMP v3 strengthens the security by adding **USM (User-based Security Mode)** and **VACM (View-based Access Control Model)**.

SNMP protocol provides a simple way of exchange network management information between two points in the network. SNMP employs a polling mechanism of message query, and transmits messages through UDP (a connectionless transport layer protocol). Therefore it is well supported by the existing computer networks.

SNMP protocol employs a station-agent mode. There are two parts in this structure: **NMS (Network**

Management Station) and Agent. NMS is the workstation on which SNMP client program is running. It is the core on the SNMP network management. Agent is the server software runs on the devices which need to be managed. NMS manages all the managed objects through Agents. The switch supports Agent function.

The communication between NMS and Agent functions in Client/Server mode by exchanging standard messages. NMS sends request and the Agent responds. There are seven types of SNMP message:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS sends queries to the Agent with Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request messages; and the Agent, upon receiving the requests, replies with Get-Response message. On some special situations, like network device ports are on Up/Down status or the network topology changes, Agents can send Trap messages to NMS to inform the abnormal events. Besides, NMS can also be set to alert to some abnormal events by enabling RMON function. When alert events are triggered, Agents will send Trap messages or log the event according to the settings. Inform-Request is mainly used for inter-NMS communication in the layered network management.

USM ensures the transfer security by well-designed encryption and authentication. USM encrypts the messages according to the user typed password. This mechanism ensures that the messages can't be viewed on transmission. And USM authentication ensures that the messages can't be changed on transmission. USM employs **DES-CBC** cryptography. And **HMAC-MD5** and **HMAC-SHA** are used for authentication.

VACM is used to classify the users' access permission. It puts the users with the same access permission in the same group. Users can't conduct the operation which is not authorized.

4.4.2 Introduction to MIB

The network management information accessed by NMS is well defined and organized in a **Management Information Base (MIB)**. MIB is pre-defined information which can be accessed by network management protocols. It is in layered and structured form. The pre-defined management information can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MID. Each MIB organizes all the available information with this tree structure. And each node on this tree contains an **OID (Object Identifier)** and a brief description about the node. OID is a set of integers divided by periods. It identifies the node and can be used to locate the node in a MID tree structure, shown in the figure below:

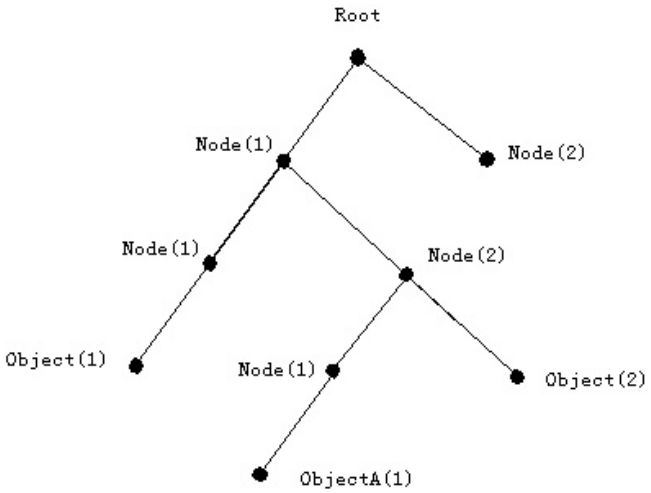


Figure 4-1 ASN.1 Tree Instance

In this figure, the OID of the object A is 1.2.1.1. NMS can locate this object through this unique OID and gets the standard variables of the object. MIB defines a set of standard variables for monitored network devices by following this structure.

If the variable information of Agent MIB needs to be browsed, the MIB browse software needs to be run on the NMS. MIB in the Agent usually consists of public MIB and private MIB. The public MIB contains public network management information that can be accessed by all NMS; private MIB contains specific information which can be viewed and controlled by the support of the manufacturers.

MIB-I [RFC1156] is the first implemented public MIB of SNMP, and is replaced by MIB-II [RFC1213]. MIB-II expands MIB-I and keeps the OID of MIB tree in MIB-I. MIB-II contains sub-trees which are called groups. Objects in those groups cover all the functional domains in network management. NMS obtains the network management information by visiting the MIB of SNMP Agent.

The switch can operate as a SNMP Agent, and supports both SNMP v1/v2c and SNMP v3. The switch supports basic MIB-II, RMON public MIB and other public MID such as BRIDGE MIB. Besides, the switch supports self-defined private MIB.

4.4.3 Introduction to RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.

- **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.4.4 SNMP Configuration

4.4.4.1 SNMP Configuration Task List

1. Enable or disable SNMP Agent server function
2. Configure SNMP community string
3. Configure IP address of SNMP management base
4. Configure engine ID
5. Configure user
6. Configure group
7. Configure view
8. Configuring TRAP
9. Enable/Disable RMON

1. Enable or disable SNMP Agent server function

Command	Explanation
Global Mode	
snmp-server enabled **no snmp-server enabled**	Enable the SNMP Agent function on the switch; the no command disables the SNMP Agent function on the switch.

2. Configure SNMP community string

Command	Explanation
Global Mode	
snmp-server community {ro|rw} <*string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}] [read <*read-view-name*>] [write <*write-view-name*>] **no snmp-server community <*string*> [access {<*num-std*>|<*name*>}] [ipv6-access {<*ipv6-num-std*>|<*ipv6-name*>}]**	Configure the community string for the switch; the no command deletes the configured community string.

3. Configure IP address of SNMP management base

Command	Explanation
Global Mode	
snmp-server securityip { *<ipv4-addr>* | *<ipv6-addr>* } **no snmp-server securityip { *<ipv4-addr>* | *<ipv6-addr>* }**	Configure the secure IPv4/IPv6 address which is allowed to access the switch on the NMS; the no command deletes configured secure address.
snmp-server securityip enable **snmp-server securityip disable**	Enable or disable secure IP address check function on the NMS.

4. Configure engine ID

Command	Explanation
Global Mode	
snmp-server engineid *<engine-string>* **no snmp-server engineid**	Configure the local engine ID on the switch. This command is used for SNMP v3.

5. Configure user

Command	Explanation
Global Mode	
snmp-server user *<use-string>* *<group-string>* [{authPriv | authNoPriv} auth {md5 | sha} *<word>*] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] **no snmp-server user *<user-string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**	Add a user to a SNMP group. This command is used to configure USM for SNMP v3.

6. Configure group

Command	Explanation
Global Mode	
snmp-server group *<group-string>* {noauthnopriv|authnopriv|authpriv} [[read *<read-string>*] [write *<write-string>*] [notify *<notify-string>*]] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] **no snmp-server group *<group-string>* {noauthnopriv|authnopriv|authpriv} [access {*<num-std>*|*<name>*}] [ipv6-access**	Set the group information on the switch. This command is used to configure VACM for SNMP v3.

{<*ipv6-num-std*>|<*ipv6-name*>}]	

7. Configure view

Command	Explanation
Global Mode	
snmp-server view <*view-string*> <*oid-string*> {include|exclude} **no snmp-server view <*view-string*>[<*oid-string*>]**	Configure view on the switch. This command is used for SNMP v3.

8. Configuring TRAP

Command	Explanation
Global Mode	
snmp-server enable traps **no snmp-server enable traps**	Enable the switch to send Trap message. This command is used for SNMP v1/v2/v3.
snmp-server host { <*ipv4-addr*> | <*ipv6-addr*> } {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} <*user-string*> **no snmp-server host { <*ipv4-addr*> | <*ipv6-addr*> } {v1 | v2c | {v3 {noauthnopriv | authnopriv | authpriv}}} <*user-string*>**	Set the host IPv4/IPv6 address which is used to receive SNMP Trap information. For SNMP v1/v2, this command also configures Trap community string; for SNMP v3, this command also configures Trap user name and security level. The “no” form of this command cancels this IPv4 or IPv6 address.

9. Enable/Disable RMON

Command	Explanation
Global mode	
rmon enable **no rmon enable**	Enable/disable RMON.

4.4.5 Typical SNMP Configuration Examples

The IP address of the NMS is 1.1.1.5; the IP address of the switch (Agent) is 1.1.1.9.

Scenario 1: The NMS network administrative software uses SNMP protocol to obtain data from the switch. The configuration on the switch is listed below:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server community rw private
Switch(config)#snmp-server community ro public
Switch(config)#snmp-server securityip 1.1.1.5
```

The NMS can use private as the community string to access the switch with read-write permission, or use public as the community string to access the switch with read-only permission.

Scenario 2: NMS will receive Trap messages from the switch (Note: NMS may have community string verification for the Trap messages. In this scenario, the NMS uses a Trap verification community string of usertrap).
The configuration on the switch is listed below:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
Switch(config)#snmp-server enable traps
```

Scenario 3: NMS uses SNMP v3 to obtain information from the switch.
The configuration on the switch is listed below:

```
Switch(config)#snmp-server
Switch(config)#snmp-server user tester UserGroup authPriv auth md5 hellotst
Switch(config)#snmp-server group UserGroup AuthPriv read max write max notify max
Switch(config)#snmp-server view max 1 include
```

Scenario 4: NMS wants to receive the v3Trap messages sent by the switch.
The configuration on the switch is listed below:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 10.1.1.2 v3 authpriv tester
Switch(config)#snmp-server enable traps
```

Scenario 5: The IPv6 address of the NMS is 2004:1:2:3::2; the IPv6 address of the switch (Agent) is 2004:1:2:3::1. The NMS network administrative software uses SNMP protocol to obtain data from the switch.
The configuration on the switch is listed below:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server community rw private
Switch(config)#snmp-server community ro public
Switch(config)#snmp-server securityip 2004:1:2:3::2
```

The NMS can use private as the community string to access the switch with read-write permission, or use public as the community string to access the switch with read-only permission.

Scenario 6: NMS will receive Trap messages from the switch (Note: NMS may have community string verification for the Trap messages. In this scenario, the NMS uses a Trap verification community string of trap).
The configuration on the switch is listed below:

```
Switch(config)#snmp-server host 2004:1:2:3::2 v1 trap
Switch(config)#snmp-server enable traps
```

4.4.6 SNMP Troubleshooting

When users configure the SNMP, the SNMP server may fail to run properly due to physical connection failure and wrong configuration, etc. Users can troubleshoot the problems by following the guide below:

- Good condition of the physical connection.
- Interface and datalink layer protocol is Up (use the “show interface” command), and the connection between the switch and host can be verified by ping (use “ping” command).
- The switch enabled SNMP Agent server function (use “snmp-server” command)
- Secure IP for NMS (use “snmp-server securityip” command) and community string (use “snmp-server community” command) are correctly configured, as any of them fails, SNMP will not be able to communicate with NMS properly.
- If Trap function is required, remember to enable Trap (use “snmp-server enable traps” command). And remember to properly configure the target host IP address and community string for Trap (use “snmp-server host” command) to ensure Trap message can be sent to the specified host.
- If RMON function is required, RMON must be enabled first (use “rmon enable” command).
- Use “show snmp” command to verify sent and received SNMP messages; Use “show snmp status” command to verify SNMP configuration information; Use “debug snmp packet” to enable SNMP debugging function and verify debug information.

If users still can’t solve the SNMP problems, Please contact our technical and service center.

4.5 Switch Upgrade

Switch provides two ways for switch upgrade: BootROM upgrade and the TFTP/FTP upgrade under Shell.

4.5.1 Switch System Files

The system files includes system image file and boot file. The updating of the switch is to update the two files by overwrite the old files with the new ones.

The system image files refers to the compressed files of the switch hardware drivers, and software support program, etc, namely what we usually call the IMG update file. The IMG file can only be saved in the FLASH with a defined name of nos.img

The boot file is for initiating the switch, namely what we usually call the ROM update file (It can be compressed into IMG file if it is of large size). The boot file can only be saved in the ROM in which the file name is defined as boot.rom

The update method of the system image file and the boot file is the same. The switch supplies the user with two modes of updating: 1. BootROM mode; 2. TFTP and FTP update at Shell mode. This two update method

will be explained in details in following two sections.

4.5.2 BootROM Upgrade

There are two methods for BootROM upgrade: TFTP and FTP, which can be selected at BootROM command settings.

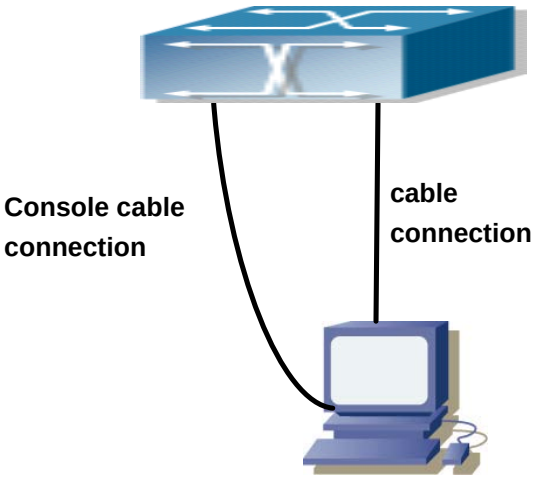


Figure 4-2 Typical topology for switch upgrade in BootROM mode

The upgrade procedures are listed below:

Step 1:

As shown in the figure, a PC is used as the console for the switch. A console cable is used to connect PC to the management port on the switch. The PC should have FTP/TFTP server software installed and has the image file required for the upgrade.

Step 2:

Press “ctrl+b” on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below:

```
[Boot]:
```

Step 3:

Under BootROM mode, run “setconfig” to set the IP address and mask of the switch under BootROM mode, server IP address and mask, and select TFTP or FTP upgrade. Suppose the switch address is 192.168.1.2, and PC address is 192.168.1.66, and select TFTP upgrade, the configuration should like:

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.2
Server IP Address: [10.1.1.2] 192.168.1.66
FTP(1) or TFTP(2): [1] 2
Network interface configure OK.
```

```
[Boot]
```

Step 4:

Enable FTP/TFTP server in the PC. For TFTP, run TFTP server program; for FTP, run FTP server program. Before start downloading upgrade file to the switch, verify the connectivity between the server and the switch by ping from the server. If ping succeeds, run “load” command in the BootROM mode from the switch; if it fails, perform troubleshooting to find out the cause. The following is the configuration for the system update image file.

```
[Boot]: load nos.img
Loading...

Loading file ok!
```

Step 5:

Execute “write nos.img” in BootROM mode. The following saves the system update image file.

```
[Boot]: write nos.img
File nos.img exists, overwrite? (Y/N)?[N] y
Writing nos.img.....................................................
Write nos.img OK.
[Boot]:
```

Step 6:

The following update file boot.rom, the basic environment is the same as Step 4.

```
[Boot]: load boot.room
Loading…

Loading file ok!
```

Step 7:

Execute “write boot.rom” in BootROM mode. The following saves the update file.

```
[Boot]: write boot.rom

File boot.rom exists, overwrite? (Y/N)?[N] y

Writing boot.rom……
Write boot.rom OK.
[Boot]:
```

Step 8:

After successful upgrade, execute run or reboot command in BootROM mode to return to CLI configuration interface.

```
[Boot]: run（or reboot）
```

Other commands in BootROM mode

1. DIR command

Used to list existing files in the FLASH .

```
[Boot]: dir
boot.rom                    327,440 1900-01-01 00:00:00 --SH
boot.conf                        83 1900-01-01 00:00:00 --SH
nos.img                   2,431,631 1980-01-01 00:21:34 ----
startup-config                2,922 1980-01-01 00:09:14 ----
temp.img                  2,431,631 1980-01-01 00:00:32 ----
```

2. CONFIG RUN command

Used to set the IMAGE file to run upon system start-up, and the configuration file to run upon configuration recovery.

```
[Boot]: config run
Boot File: [nos.img] nos.img
Config File: [boot.conf]
```

4.5.3 FTP/TFTP Upgrade

4.5.3.1 Introduction to FTP/TFTP

FTP(File Transfer Protocol)/TFTP(Trivial File Transfer Protocol) are both file transfer protocols that belonging to fourth layer(application layer) of the TCP/IP protocol stack, used for transferring files between hosts, hosts and switches. Both of them transfer files in a client-server model. Their differences are listed below.

FTP builds upon TCP to provide reliable connection-oriented data stream transfer service. However, it does not provide file access authorization and uses simple authentication mechanism (transfers username and password in plain text for authentication). When using FTP to transfer files, two connections need to be established between the client and the server: a management connection and a data connection. A transfer request should be sent by the FTP client to establish management connection on port 21 in the server, and negotiate a data connection through the management connection.

There are two types of data connections: active connection and passive connection.

In active connection, the client transmits its address and port number for data transmission to the server, the

management connection maintains until data transfer is complete. Then, using the address and port number provided by the client, the server establishes data connection on port 20 (if not engaged) to transfer data; if port 20 is engaged, the server automatically generates some other port number to establish data connection.

In passive connection, the client, through management connection, notify the server to establish a passive connection. The server then creates its own data listening port and informs the client about the port, and the client establishes data connection to the specified port.

As data connection is established through the specified address and port, there is a third party to provide data connection service.

TFTP builds upon UDP, providing unreliable data stream transfer service with no user authentication or permission-based file access authorization. It ensures correct data transmission by sending and acknowledging mechanism and retransmission of time-out packets. The advantage of TFTP over FTP is that it is a simple and low overhead file transfer service.

Switch can operate as either FTP/TFTP client or server. When switch operates as a FTP/TFTP client, configuration files or system files can be downloaded from the remote FTP/TFTP servers (can be hosts or other switches) without affecting its normal operation. And file list can also be retrieved from the server in ftp client mode. Of course, switch can also upload current configuration files or system files to the remote FTP/TFTP servers (can be hosts or other switches). When switch operates as a FTP/TFTP server, it can provide file upload and download service for authorized FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

- **ROM:** Short for EPROM, erasable read-only memory. EPROM is repalced by FLASH memory in switch.
- **SDRAM:** RAM memory in the switch, used for system software operation and configuration sequence storage.
- **FLASH:** Flash memory used to save system file and configuration file.
- **System file:** including system image file and boot file.
- **System image file:** refers to the compressed file for switch hardware driver and software support program, usually refer to as IMAGE upgrade file. In switch, the system image file is allowed to save in FLASH only. Switch mandates the name of system image file to be uploaded via FTP in Global Mode to be nos.img, other IMAGE system files will be rejected.
- **Boot file:** refers to the file initializes the switch, also referred to as the ROM upgrade file (Large size file can be compressed as IMAGE file). In switch, the boot file is allowed to save in ROM only. Switch mandates the name of the boot file to be boot.rom.
- **Configuration file:** including start up configuration file and running configuration file. The distinction between start up configuration file and running configuration file can facilitate the backup and update of the configurations.
- **Start up configuration file:** refers to the configuration sequence used in switch start up. Switch start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, switch mandates the name of start up configuration file to be startup-config.

- **Running configuration file:** refers to the running configuration sequence use in the switch. In switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by **write** command or **copy running-config startup-config** command, so that the running configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, switch mandates the name of running configuration file to be running-config.
- **Factory configuration file:** The configuration file shipped with switch in the name of factory-config. Run set default and write, and restart the switch, factory configuration file will be loaded to overwrite current start up configuration file.

4.5.3.2 FTP/TFTP Configuration

The configurations of switch as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

4.5.3.2.1 FTP/TFTP Configuration Task List

1. FTP/TFTP client configuration
   （1） Upload/download the configuration file or system file.
   （2） For FTP client, server file list can be checked.
2. FTP server configuration
   （1）Start FTP server
   （2）Configure FTP login username and password
   （3）Modify FTP server connection idle time
   （4）Shut down FTP server
3. TFTP server configuration
   （1）Start TFTP server
   （2）Configure TFTP server connection idle time
   （3）Configure retransmission times before timeout for packets without acknowledgement
   （4）Shut down TFTP server

1. FTP/TFTP client configuration

（1）FTP/TFTP client upload/download file

Command	Explanation
Admin Mode	
copy <*source-url*> <*destination-url*> [ascii | binary]	FTP/TFTP client upload/download file.

（2）For FTP client, server file list can be checked.

Admin Mode	

ftp-dir <*ftpServerUrl*>	For FTP client, server file list can be checked. FtpServerUrl format looks like: ftp: //user: password@IPv4|IPv6 Address.

2. FTP server configuration

（1）Start FTP server

Command	Explanation
Global Mode	
ftp-server enable **no ftp-server enable**	Start FTP server and support IPv4, IPv6, the no command shuts down FTP server and prevents FTP user from logging in.

（2）Configure FTP login username and password

Command	Explanation
Global Mode	
ip ftp username <*username*> **{nopassword | password {0 | 7}** **<*password*>}** **no ip ftp username<*username*>**	Configure FTP login username and password; this no command will delete the username and password.

（3）Modify FTP server connection idle time

Command	Explanation
Global Mode	
ftp-server timeout <*seconds*>	Set connection idle time.

3. TFTP server configuration

（1）Start TFTP server

Command	Explanation
Global Mode	
tftp-server enable **no tftp-server enable**	Start TFTP server, the no command shuts down TFTP server and prevents TFTP user from logging in.

（2）Modify TFTP server connection idle time

Command	Explanation

Global Mode	
tftp-server retransmission-timeout <*seconds*>	Set maximum retransmission time within timeout interval.

（3）Modify TFTP server connection retransmission time

Command	Explanation
Global Mode	
tftp-server retransmission-number <*number*>	Set the retransmission time for TFTP server.

4.5.3.3 FTP/TFTP Configuration Examples

It is the same configuration switch for IPv4 addresses and IPv6 addresses. The example only for the IPv4 addresses configuration.

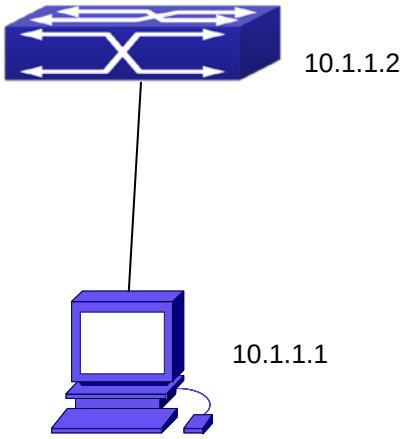


Figure 4-3 Download nos.img file as FTP/TFTP client

Scenario 1: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; the switch acts as a FTP/TFTP client, the IP address of the switch management VLAN is 10.1.1.2. Download “nos.img” file in the computer to the switch.

- FTP Configuration

Computer side configuration:

Start the FTP server software on the computer and set the username “Switch”, and the password “switch”. Place the “12_30_nos.img” file to the appropriate FTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#exit
Switch#copy ftp: //Switch:switch@10.1.1.1/12_30_nos.img nos.img
```

With the above commands, the switch will have the “nos.img” file in the computer downloaded to the FLASH.

- TFTP Configuration

Computer side configuration:

Start TFTP server software on the computer and place the “nos.img” file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#exit
Switch#copy tftp: //10.1.1.1/12_30_nos.img nos.img
```

Scenario 2: The switch is used as FTP server. The switch operates as the FTP server and connects from one of its ports to a computer, which is a FTP client. Transfer the “nos.img” file in the switch to the computer and save as 12_25_nos.img.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#ftp-server enable
Switch(config)# username Admin password 0 switch
```

Computer side configuration:

Login to the switch with any FTP client software, with the username “Admin” and password “switch”, use the command “get nos.img 12_25_nos.img” to download “nos.img” file from the switch to the computer.

Scenario 3: The switch is used as TFTP server. The switch operates as the TFTP server and connects from one of its ports to a computer, which is a TFTP client. Transfer the “nos.img” file in the switch to the computer.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#tftp-server enable
```

Computer side configuration:

Login to the switch with any TFTP client software, use the “tftp” command to download “nos.img” file from the switch to the computer.

Scenario 4: Switch acts as FTP client to view file list on the FTP server.
Synchronization conditions: The switch connects to a computer by an Ethernet port, the computer is a FTP server with an IP address of 10.1.1.1; the switch acts as a FTP client, and the IP address of the switch management VLAN1 interface is 10.1.1.2.

- FTP Configuration

PC side:
Start the FTP server software on the PC and set the username “Switch”, and the password “Admin”.
Switch:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch#copy ftp: //Switch: superuser@10.1.1.1
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
…(some display omitted here)
show.txt
snmp.TXT
226 Transfer complete.
```

4.5.3.4 FTP/TFTP Troubleshooting

4.5.3.4.1 FTP Troubleshooting

When upload/download system file with FTP protocol, the connectivity of the link must be ensured, i.e., use the “Ping” command to verify the connectivity between the FTP client and server before running the FTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

- The following is what the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry “copy” command again.

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
nos.img file length = 1526021
read file ok
send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.
```

- The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry “copy” command again.

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
recv total = 1526037
**************************
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.
```

- If the switch is upgrading system file or system start up file through FTP, the switch must not be restarted until “close ftp client” or “226 Transfer complete.” is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through FTP fails, please try to upgrade again or use the BootROM mode to upgrade.

4.5.3.4.2 TFTP Troubleshooting

When upload/download system file with TFTP protocol, the connectivity of the link must be ensured, i.e., use the "**Ping**" command to verify the connectivity between the TFTP client and server before running the TFTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

- The following is the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry "copy" command again.

```
nos.img file length = 1526021
read file ok
begin to send file, wait...
file transfers complete.
Close tftp client.
```

- The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry "copy" command again.

```
begin to receive file, wait...
recv 1526037
**********
write ok
transfer complete
close tftp client.
```

If the switch is upgrading system file or system start up file through TFTP, the switch must not be restarted until "close tftp client" is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through TFTP fails, please try upgrade again or use the BootROM mode to upgrade.

Chapter 5 Cluster Configuration

5.1 Introduction to cluster network management

Cluster network management is an in-band configuration management. Unlike CLI, SNMP and Web Config which implement a direct management of the target switches through a management workstation, cluster network management implements a direct management of the target switches (member switches) through an intermediate switch (commander switch). A commander switch can manage multiple member switches. As soon as a Public IP address is configured in the commander switch, all the member switches which are configured with private IP addresses can be managed remotely. This feature economizes public IP addresses which are short of supply. Cluster network management can dynamically discover cluster feature enabled switches (candidate switches). Network administrators can statically or dynamically add the candidate switches to the cluster which is already established. Accordingly, they can configure and manage the member switches through the commander switch. When the member switches are distributed in various physical locations (such as on the different floors of the same building), cluster network management has obvious advantages. Moreover, cluster network management is an in-band management. The commander switch can communicate with member switches in existing network. There is no need to build a specific network for network management.

Cluster network management has the following features:

- Save IP addresses
- Simplify configuration tasks
- Indifference to network topology and distance limitation
- Auto detecting and auto establishing
- With factory default settings, multiple switches can be managed through cluster network management
- The commander switch can upgrade and configure any member switches in the cluster

5.2 Cluster Network Management Configuration Sequence

Cluster Network Management Configuration Sequence:

1 · Enable or disable cluster function

2 · Create cluster

   1) Configure private IP address pool for member switches of the cluster
   2) Create or delete cluster
   3) Add or remove a member switch

3 · Configure attributes of the cluster in the commander switch

   1) Enable or disable automatically adding cluster members
   2) Set automatically added members to manually added ones
   3) Set or modify the time interval of keep-alive messages on switches in the cluster.
   4) Set or modify the max number of lost keep-alive messages that can be tolerated

5) Clear the list of candidate switches maintained by the switch

4 · Configure attributes of the cluster in the candidate switch

1) Set the time interval of keep-alive messages of the cluster

2) Set the max number of lost keep-alive messages that can be tolerated in the cluster

5 · Remote cluster network management

1) Remote configuration management

2) Remotely upgrade member switch

3) Reboot member switch

6 · Manage cluster network with web

1) Enable http

7 · Manage cluster network with snmp

1) Enable snmp server

1. Enable or disable cluster

Command	Explanation
Global Mode	
cluster run [key <*WORD*>] [vid <*VID*>] **no cluster run**	Enable or disable cluster function in the switch.

2. Create a cluster

Command	Explanation
Global Mode	
cluster ip-pool <*commander-ip*> **no cluster ip-pool**	Configure the private IP address pool for cluster member devices.
cluster commander [<*cluster_name*>] **no cluster commander**	Create or delete a cluster.
cluster member {candidate-sn <*candidate-sn*> **| mac-address <*mac-addr*> [id <*member-id*>]}** **no cluster member {id <*member-id*> |** **mac-address <*mac-addr*>}**	Add or remove a member switch.

3. Configure attributes of the cluster in the commander switch

Command	Explanation
Global Mode	
cluster auto-add **no cluster auto-add**	Enable or disable adding newly discovered candidate switch to the cluster.
cluster member auto-to-user	Change automatically added members into manually added ones.
cluster keepalive interval <*second*> **no cluster keepalive interval**	Set the keep-alive interval of the cluster.

cluster keepalive loss-count <*int*> **no cluster keepalive loss-count**	Set the max number of lost keep-alive messages that can be tolerated in the cluster.
Admin mode	
clear cluster nodes [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]	Clear nodes in the list of candidate switches maintained by the switch.

4. Configure attributes of the cluster in the candidate switch

Command	Explanation
Global Mode	
cluster keepalive interval <*second*> **no cluster keepalive interval**	Set the keep-alive interval of the cluster.
cluster keepalive loss-count <*int*> **no cluster keepalive loss-count**	Set the max number of lost keep-alive messages that can be tolerated in the clusters.

5. Remote cluster network management

Command	Explanation
Admin Mode	
rcommand member <*member-id*>	In the commander switch, this command is used to configure and manage member switches.
rcommand commander	In the member switch, this command is used to configure the commander switch.
cluster reset member [id <*member-id*> | mac-address <*mac-addr*>]	In the commander switch, this command is used to reset the member switch.
cluster update member <*member-id*> <*src-url*> <*dst-filename*>[ascii | binary]	In the commander switch, this command is used to remotely upgrade the member switch. It can only upgrade nos.img file.

6. Manage cluster network with web

Command	Explanation
Global Mode	
ip http server	Enable http function in commander switch and member switch. Notice: must insure the http function be enabled in member switch when commander switch visiting member switch by web. The commander switch visit member switch via beat member node in member cluster topology.

7. Manage cluster network with snmp

Command	Explanation
Global Mode	
snmp-server enable	Enable snmp server function in commander switch and member switch. Notice: must insure the snmp server function be enabled in member switch when commander switch visiting member switch by snmp. The commander switch visit member switch via configure character string <commander-community>@sw<member id>.

5.3 Examples of Cluster Administration

Scenario:

The four switches SW1-SW4, amongst the SW1 is the command switch and other switches are member switch. The SW2 and SW4 is directly connected with the command switch, SW3 connects to the command switch through SW2.

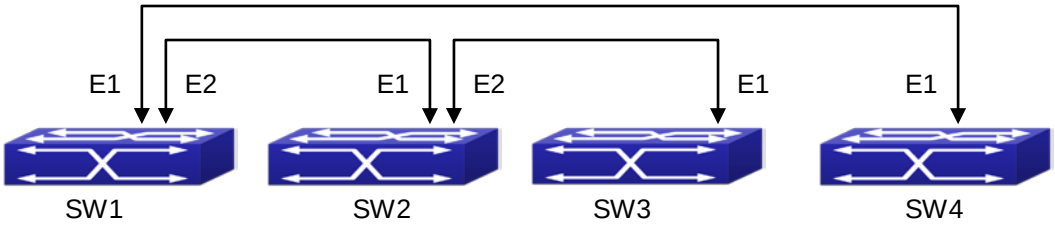


Figure 5-1 Examples of Cluster

Configuration Procedure

1. Configure the command switch

Configuration of SW1:

```
Switch(config)#cluster run
Switch(config)#cluster ip-pool 10.2.3.4
Switch(config)#cluster commander 5526
Switch(config)#cluster auto-add
```

2. Configure the member switch

Configuration of SW2-SW4

```
Switch(config)#cluster run
```

5.4 Cluster Administration Troubleshooting

When encountering problems in applying the cluster admin, please check the following possible causes:

- If the command switch is correctly configured and the auto adding function (cluster auto-add) is enabled. If the ports connected the command switch and member switch belongs to the cluster vlan.
- After cluster commander is enabled in VLAN1 of the command switch, please don't enable a routing protocol (RIP, OSPF, BGP) in this VLAN in order to prevent the routing protocol from broadcasting the private cluster addresses in this VLAN to other switches and cause routing loops.
- Whether the connection between the command switch and the member switch is correct. We can use the debug cluster packets to check if the command and the member switches can receive and process related cluster admin packets correctly.

Chapter 6 Port Configuration

6.1 Introduction to Port

Switch contain Cable ports and Combo ports. The Combo ports can be configured to as either 1000GX-TX ports or SFP Gigabit fiber ports.

If the user needs to configure some network ports, he/she can use the interface ethernet <interface-list> command to enter the appropriate Ethernet port configuration mode, where <interface-list> stands for one or more ports. If <interface-list> contains multiple ports, special characters such as ';' or '-' can be used to separate ports, ';' is used for discrete port numbers and '-' is used for consecutive port numbers. Suppose an operation should be performed on ports 2, 3, 4, 5, the command would look like: interface ethernet 1/2-5. Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

6.2 Network Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   (1) Configure combo mode for combo ports
   (2) Enable/Disable ports
   (3) Configure port names
   (4) Configure port cable types
   (5) Configure port speed and duplex mode
   (6) Configure bandwidth control
   (7) Configure traffic control
   (8) Enable/Disable port loopback function
   (9) Configure broadcast storm control function for the switch
   (10) Configure scan port mode

1. Enter the Ethernet port configuration mode

Command	**Explanation**
Global Mode	
interface ethernet *<interface-list>*	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	**Explanation**
Port Mode	
combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto }	Sets the combo port mode (combo ports only).

shutdown **no shutdown**	Enables/Disables specified ports.
name <*string*> **no name**	Names or cancels the name of specified ports.
mdi {auto | across | normal} **no mdi**	Sets the cable type for the specified port; this command is not supported by combo port and fiber port of switch.
speed-duplex {auto | force10-half | force10-full | force100-half | force100-full |force100-fx | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }	Sets port speed and duplex mode of 100/1000Base-TX or 100Base-FX ports. The no format of this command restores the default setting, i.e., negotiates speed and duplex mode automatically.
negotiation {on|off}	Enables/Disables the auto-negotiation function of 1000Base-FX ports.
bandwidth control <*bandwidth*> [both | receive | transmit] **no bandwidth control**	Sets or cancels the bandwidth used for incoming/outgoing traffic for specified ports.
flow control **no flow control**	Enables/Disables traffic control function for specified ports.
loopback **no loopback**	Enables/Disables loopback test function for specified ports.
rate-suppression {dlf | broadcast | multicast} <packets>	Enables the storm control function for broadcasts, multicasts and unicasts with unknown destinations (short for broadcast), and sets the allowed broadcast packet number; the no format of this command disables the broadcast storm control function.
port-scan-mode {interrupt | poll} **no port-scan-mode**	Configure port-scan-mode as interrupt or poll mode, the no command restores the default port-scan-mode.

6.3 Port Configuration Example

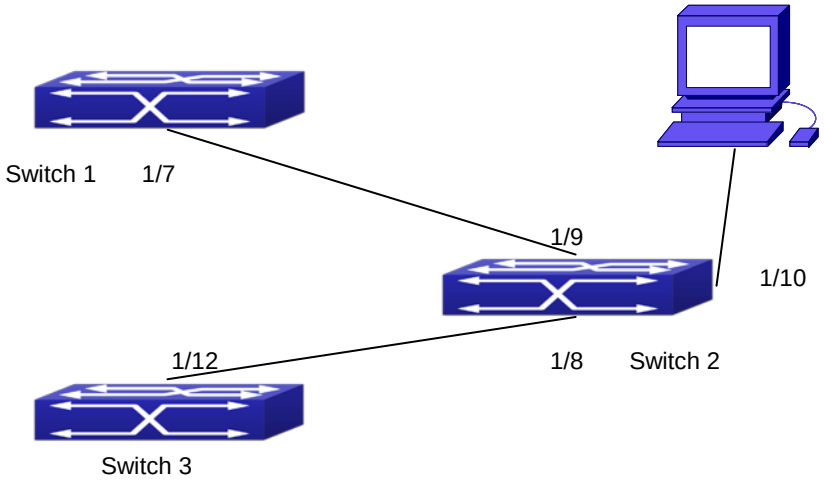


Figure 6-1 Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

Switch	Port	Property
Switch1	1/7	Ingress bandwidth limit: 150 M
Switch2	1/8	Mirror source port
	1/9	100Mbps full, mirror source port
	1/10	1000Mbps full, mirror destination port
Switch3	1/12	100Mbps full

The configurations are listed below:

Switch1:

```
Switch1(config)#interface ethernet 1/7
Switch1(Config-If-Ethernet1/7)#bandwidth control 50 both
```

Switch2:

```
Switch2(config)#interface ethernet 1/9
Switch2(Config-If-Ethernet1/9)#speed-duplex force100-full
Switch2(Config-If-Ethernet1/9)#exit
Switch2(config)#interface ethernet 1/10
Switch2(Config-If-Ethernet1/10)# speed-duplex force1000-full
Switch2(Config-If-Ethernet1/10)#exit
Switch2(config)#monitor session 1 source interface ethernet1/8;1/9
Switch2(config)#monitor session 1 destination interface ethernet 1/10
```

Switch3:

```
Switch3(config)#interface ethernet 1/12
Switch3(Config-If-Ethernet1/12)#speed-duplex force1000-full
Switch3(Config-If-Ethernet1/12)#exit
```

6.4 Port Troubleshooting

Here are some situations that frequently occurs in port configuration and the advised solutions:

- Two connected fiber interfaces won't link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance.

Chapter 7 Port Loopback Detection Function Configuration

7.1 Introduction to Port Loopback Detection Function

With the development of switches, more and more users begin to access the network through Ethernet switches. In enterprise network, users access the network through layer-2 switches, which means urgent demands for both internet and the internal layer 2 Interworking. When layer 2 Interworking is required, the messages will be forwarded through MAC addressing the accuracy of which is the key to a correct Interworking between users. In layer 2 switching, the messages are forwarded through MAC addressing. Layer 2 devices learn MAC addresses via learning source MAC address, that is, when the port receives a message from an unknown source MAC address, it will add this MAC to the receive port, so that the following messages with a destination of this MAC can be forwarded directly, which also means learn the MAC address once and for all to forward messages.

When a new source MAC is already learnt by the layer 2 device, only with a different source port, the original source port will be modified to the new one, which means to correspond the original MAC address with the new port. As a result, if there is any loopback existing in the link, all MAC addresses within the whole layer 2 network will be corresponded with the port where the loopback appears (usually the MAC address will be frequently shifted from one port to another), causing the layer 2 network collapsed. That is why it is a necessity to check port loopbacks in the network. When a loopback is detected, the detecting device should send alarms to the network management system, ensuring the network manager is able to discover, locate and solve the problem in the network and protect users from a long-lasting disconnected network.

Since detecting loopbacks can make dynamic judgment of the existence of loopbacks in the link and tell whether it has gone, the devices supporting port control (such as port isolation and port MAC address learning control) can maintain that automatically, which will not only reduce the burden of network managers but also response time, minimizing the effect caused loopbacks to the network.

7.2 Port Loopback Detection Function Configuration Task List

1. Configure the time interval of loopback detection
2. Enable the function of port loopback detection
3. Configure the control method of port loopback detection
4. Display and debug the relevant information of port loopback detection
5. Configure the loopback-detection control mode (automatic recovery enabled or not)

1． Configure the time interval of loopback detection

Command	**Explanation**
Global Mode	

loopback-detection interval-time *<loopback> <no-loopback>* **no loopback-detection interval-time**	Configure the time interval of loopback detection.

2 · Enable the function of port loopback detection

Command	**Explanation**
Global Mode	
loopback-detection specified-vlan <vlan-*list*> **no loopback-detection specified-vlan <vlan-*list*>**	Enable and disable the function of port loopback detection.

3 · Configure the control method of port loopback detection

Command	**Explanation**
Global Mode	
loopback-detection control {shutdown |block| learning} **no loopback-detection control**	Enable and disable the function of port loopback detection control.

4 · Display and debug the relevant information of port loopback detection

Command	**Explanation**
Global Mode	
debug loopback-detection **no debug loopback-detection**	Enable the debug information of the function module of port loopback detection. The no operation of this command will disable the debug information.
show loopback-detection [interface *<interface-list>*]	Display the state and result of the loopback detection of all ports, if no parameter is provided; otherwise, display the state and result of the corresponding ports.

5 · Configure the loopback-detection control mode (automatic recovery enabled or not)

Command	**Explanation**
Global Mode	
loopback-detection control-recovery timeout <0-3600>	Configure the loopback-detection control mode (automatic recovery enabled or not) or recovery time.

7.3 Port Loopback Detection Function Example

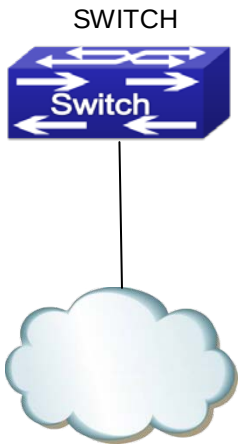


Figure 7-1 A typical example of port loopback detection

As shown in the above configuration, the switch will detect the existence of loopbacks in the network topology. After enabling the function of loopback detection on the port connecting the switch with the outside network, the switch will notify the connected network about the existence of a loopback, and control the port on the switch to guarantee the normal operation of the whole network.

The configuration task sequence of SWITCH:

```
Switch(config)#loopback-detection interval-time 35 15
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#loopback-detection special-vlan 1-3
Switch(Config-If-Ethernet1/1)#loopback-detection control block
```

If adopting the control method of block, MSTP should be globally enabled. And the correspondence between the spanning tree instance and the VLAN should be configured.

```
Switch(config)#spanning-tree
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#instance 2 vlan 2
Switch(Config-Mstp-Region)#
```

7.4 Port Loopback Detection Troubleshooting

The function of port loopback detection is disabled by default and should only be enabled if required.

Chapter 8 Port Channel Configuration

8.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level; only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) with the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

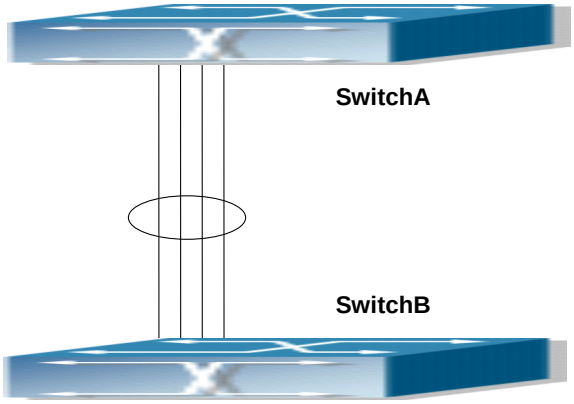


Figure 8-1 Port aggregation

As shown in the above, SwitchA is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from SwitchA needs to be transferred to SwitchB through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address. The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

Switch offers two methods for configuring port aggregation: manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full-duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as follows:

- All ports are in full-duplex mode.
- All Ports are of the same speed.
- All ports are Access ports and belong to the same VLAN or are all TRUNK ports, or are all Hybrid ports.
- If the ports are all TRUNK ports, then their "Allowed VLAN" and "Native VLAN" property should also be

the same.

If Port Channel is configured manually or dynamically on switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. Switch allow physical port aggregation of any two switches, maximum 8 port groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. Switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical port configuration mode.

8.2 Port Channel Configuration Task List

1. Create a port group in Global Mode.
2. Add ports to the specified group from the Port Mode of respective ports.
3. Enter port-channel configuration mode.

1. Creating a port group

Command	Explanation
Global Mode	
port-group <*port-group-number*> **[load-balance { src-mac | dst-mac |** **dst-src-mac | src-ip| dst-ip|dst-src-ip}]** **no port-group <port-group-number>** **[load-balance]**	Creates or deletes a port group and sets the load balance method for that group.

2. Add physical ports to the port group

Command	Explanation
Port Mode	
port-group *<port-group-number>* mode {active | passive | on} **no port-group <*port-group-number*>**	Adds ports to the port group and sets their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel	Enters port-channel configuration mode.

<port-channel-number>	

8.3 Port Channel Examples

Scenario 1: Configuring Port Channel in LACP.

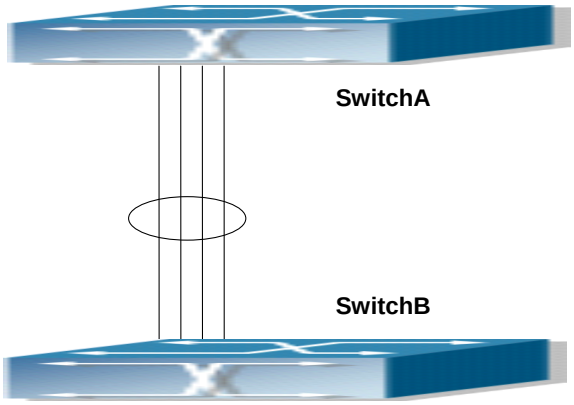


Figure 8-2 Configuring Port Channel in LACP

The switches in the description below are all switch and as shown in the figure, ports 1, 2, 3, 4 of SwitchA are access ports that belong to VLAN1. Add those four ports to group1 in active mode. Ports 6, 8, 9, 10 of SwitchB are access ports that also belong to VLAN1. Add these four ports to group2 in passive mode. All the ports should be connected with cables.

The configuration steps are listed below:

```
SwitchA#config
SwitchA (config)#interface ethernet 1/1-4
SwitchA (Config-If-Port-Range)#port-group 1 mode active
SwitchA (Config-If-Port-Range)#exit
SwitchA (config)#interface port-channel 1
SwitchA (Config-If-Port-Channel1)#

SwitchB#config
SwitchB (config)#port-group 2
SwitchB (config)#interface ethernet 1/6
SwitchB (Config-If-Ethernet1/6)#port-group 2 mode passive
SwitchB (Config-If-Ethernet1/6)#exit
SwitchB (config)#interface ethernet 1/8-10
SwitchB (Config-If-Port-Range)#port-group 2 mode passive
SwitchB (Config-If-Port-Range)#exit
SwitchB (config)#interface port-channel 2
SwitchB (Config-If-Port-Channel2)#
```

Configuration result:

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3, 4 of Switch A form an aggregated port named “Port-Channel1”, ports 6, 8, 9, 10 of Switch B forms an aggregated port named “Port-Channel2”; configurations can be made in their respective aggregated port configuration mode.

Scenario 2: Configuring Port Channel in ON mode.

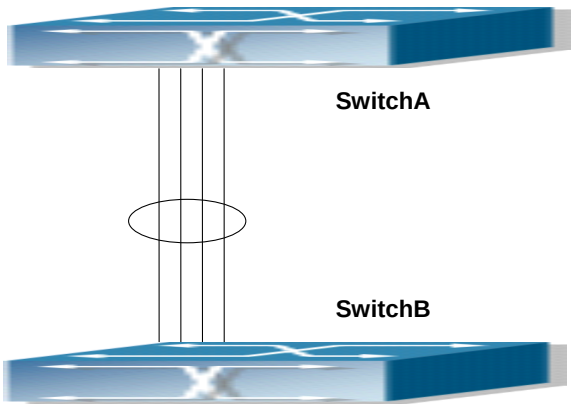


Figure 8-3 Configuring Port Channel in ON mode

Example: As shown in the figure, ports 1, 2, 3, 4 of SwitchA are access ports that belong to VLAN1. Add those four ports to group1 in “on” mode. Ports 6, 8, 9, 10 of SwitchB are access ports that also belong to VLAN1, add these four ports to group2 in “on” mode.

The configuration steps are listed below:

```
SwitchA#config
SwitchA (config)#interface ethernet 1/1
SwitchA (Config-If-Ethernet1/1)#port-group 1 mode on
SwitchA (Config-If-Ethernet1/1)#exit
SwitchA (config)#interface ethernet 1/2
SwitchA (Config-If-Ethernet1/2)#port-group 1 mode on
SwitchA (Config-If-Ethernet1/2)#exit
SwitchA (config)#interface ethernet 1/3
SwitchA (Config-If-Ethernet1/3)#port-group 1 mode on
SwitchA (Config-If-Ethernet1/3)#exit
SwitchA (config)#interface ethernet 1/4
SwitchA (Config-If-Ethernet1/4)#port-group 1 mode on
SwitchA (Config-If-Ethernet1/4)#exit

SwitchB#config
SwitchB (config)#port-group 2
SwitchB (config)#interface ethernet 1/6
SwitchB (Config-If-Ethernet1/6)#port-group 2 mode on
SwitchB (Config-If-Ethernet1/6)#exit
SwitchB (config)#interface ethernet 1/8-10
SwitchB (Config-If-Port-Range)#port-group 2 mode on
```

```
SwitchB (Config-If-Port-Range)#exit
```

Configuration result:

Add ports 1, 2, 3, 4 of Switch 1 to port-group 1 in order, and we can see a group in “on” mode is completely joined forcedly, switch in other ends won’t exchange LACP BPDU to complete aggregation. Aggregation finishes immediately when the command to add port 2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 3 joins port-group 1, port-channel 1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel 1, when port 4 joins port-group 1, port-channel 1 of port 1, 2 and 3 are ungrouped and re-aggregate with port 4 to form port-channel 1. (It should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group.) Now all four ports in both SwitchA and SwitchB are aggregated in “on” mode and become an aggregated port respectively.

8.4 Port Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

- Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.

Chapter 9 Jumbo Configuration

9.1 Introduction to Jumbo

So far the Jumbo (Jumbo Frame) has not reach a determined standard in the industry (including the format and length of the frame). Normally frames sized within 1519-9000 should be considered jumbo frame. Networks with jumbo frames will increase the speed of the whole network by 2% to 5%. Technically the Jumbo is just a lengthened frame sent and received by the switch. However considering the length of Jumbo frames, they will not be sent to CPU. We discarded the Jumbo frames sent to CPU in the packet receiving process.

9.2 Jumbo Configuration Task Sequence

1. Configure enable Jumbo function

Command	Explanation
Global Mode	
jumbo enable [<mtu-value>] **no jumbo enable**	Enable sending/receiving function of the Jumbo frames. The no command disables sending and receiving function of the Jumbo frames.

Chapter 10 VLAN Configuration

10.1 VLAN Configuration

10.1.1 Introduction to VLAN

VLAN (Virtual Local Area Network) is a technology that divides the logical addresses of devices within the network to separate network segments basing on functions, applications or management requirements. By this way, virtual workgroups can be formed regardless of the physical location of the devices. IEEE announced IEEE 802.1Q protocol to direct the standardized VLAN implementation, and the VLAN function of switch is implemented following IEEE 802.1Q.

The key idea of VLAN technology is that a large LAN can be partitioned into many separate broadcast domains dynamically to meet the demands.

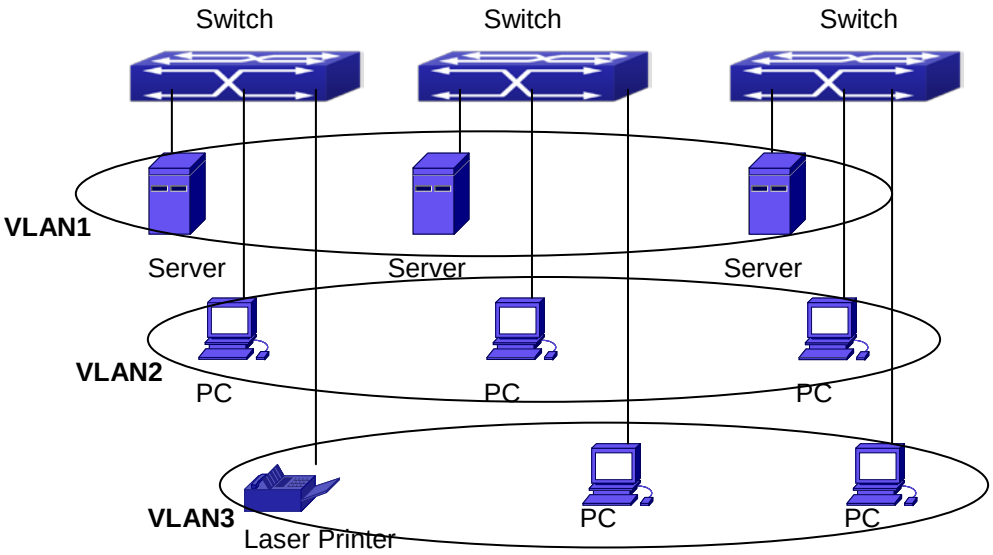


Figure 10-1 A VLAN network defined logically

Each broadcast domain is a VLAN. VLANs have the same properties as the physical LANs, except VLAN is a logical partition rather than physical one. Therefore, the partition of VLANs can be performed regardless of physical locations, and the broadcast, multicast and unicast traffic within a VLAN is separated from the other VLANs.

With the aforementioned features, VLAN technology provides us with the following convenience:

- Improving network performance
- Saving network resources
- Simplifying network management
- Lowering network cost
- Enhancing network security

The switch implements VLAN and GVRP (GARP VLAN Registration Protocol) which are defined by 802.1Q. The chapter will explain the use and the configuration of VLAN and GVRP in detail.

10.1.2 VLAN Configuration Task List

1. Create or delete VLAN
2. Set or delete VLAN name
3. Assign Switch ports for VLAN
4. Set the switch port type
5. Set Trunk port
6. Set Access port
7. Enable/Disable VLAN ingress rules on ports
8. Configure Private VLAN
9. Set Private VLAN association

1. Create or delete VLAN

Command	Explanation
Global Mode	
vlan WORD **no vlan WORD**	Create/delete VLAN or enter VLAN Mode

2. Set or delete VLAN name

Command	Explanation
Global Mode	
name <vlan-name> **no name**	Set or delete VLAN name.

3. Assigning Switch ports for VLAN

Command	Explanation
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Assign Switch ports to VLAN.

4. Set the Switch Port Type

Command	Explanation
Port Mode	
switchport mode {trunk | access}	Set the current port as Trunk or Access port.

5. Set Trunk port

Command	Explanation
Port Mode	
switchport trunk allowed vlan {WORD | all | add WORD | except WORD|remove WORD} **no switchport trunk allowed vlan**	Set/delete VLAN allowed to be crossed by Trunk. The "no" command restores the default setting.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Set/delete PVID for Trunk port.

6. Set Access port

Command	Explanation
Port Mode	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Add the current port to the specified VLAN. The "no" command restores the default setting.

7. Disable/Enable VLAN Ingress Rules

Command	Explanation
Port Mode	
vlan ingress enable **no vlan ingress enable**	Enable/Disable VLAN ingress rules.

8. Configure Private VLAN

Command	Explanation
VLAN mode	
private-vlan {primary | isolated | community} **no private-vlan**	Configure current VLAN to Private VLAN. The no command deletes private VLAN.

9. Set Private VLAN association

Command	Explanation
VLAN mode	
private-vlan association <*secondary-vlan-list*> **no private-vlan association**	Set/delete Private VLAN association.

10.1.3 Typical VLAN Application

Scenario:

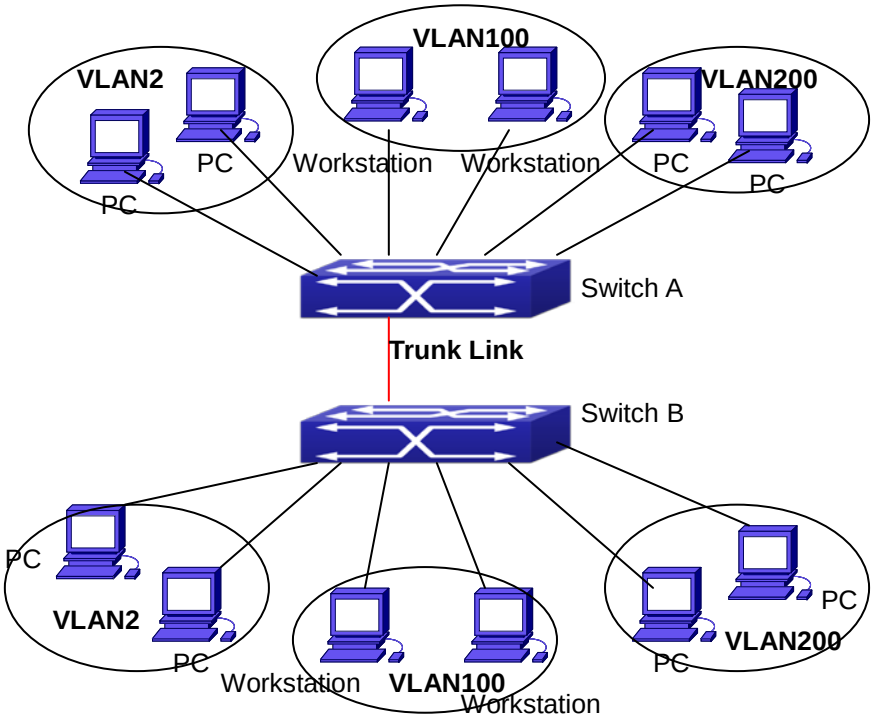


Figure 10-2 Typical VLAN Application Topology

The existing LAN is required to be partitioned to 3 VLANs due to security and application requirements. The three VLANs are VLAN2, VLAN100 and VLAN200. Those three VLANs are cross two different location A and B. One switch is placed in each site, and cross-location requirement can be met if VLAN traffic can be transferred between the two switches.

Configuration Item	Configuration description
VLAN2	Site A and site B switch port 2 -4.
VLAN100	Site A and site B switch port 5 -7.
VLAN200	Site A and site B switch port 8 -10.
Trunk port	Site A and site B switch port 11.

Connect the Trunk ports of both switches for a Trunk link to convey the cross-switch VLAN traffic; connect all network devices to the other ports of corresponding VLANs.

In this example, port 1 and port 12 is spared and can be used for management port or for other purposes.

The configuration steps are listed below:

Switch A:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
```

```
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(config)#interface ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)#exit
Switch(config)#
```

Switch B:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(config)#interface ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)#exit
```

10.2 GVRP Configuration

10.2.1 Introduction to GVRP

GARP (Generic Attribute Registration Protocol) can be used to dynamically distribute, populate and register property information between switch members within a switch network, the property can be VLAN information, Multicast MAC address of the other information. As a matter of fact, GARP protocol can convey multiple property features the switch need to populate. Various GARP applications are defined on the basis of GARP, which are called GARP application entities, and GVRP is one of them.

GVRP (GARP VLAN Registration Protocol) is an application based on GARP working mechanism. It is responsible for the maintenance of dynamic VLAN register information and population of such register information to the other switches. Switches support GVRP can receive VLAN dynamic register information from the other switches, and update local VLAN register information according the information received. The switch enabled GVRP can also populate their own VLAN register information to the other switches. The populated VLAN register information includes local static information manually configured and dynamic information learnt from the other switches. Therefore, by populating the VLAN register information, VLAN information consistency can be achieved among all GVRP enabled switches.

10.2.2 GVRP Configuration Task List

1. Configuring GARP Timer parameters

Command	Explanation
Port Mode	
garp timer join <timer-value> **no garp timer join** **garp timer leave <timer-value>** **no garp timer leave** **garp timer hold <timer-value>** **no garp timer hold**	Configure the hold, join and leave timers for GARP.
Global Mode	
garp timer leaveall <timer-value> **no garp timer leaveall**	Configure the leave all timer for GARP.

2. Enable GVRP function

Command	Explanation
Port Mode	
gvrp **no gvrp**	Enable/disable the GVRP function on current port.
Global Mode	
gvrp **no gvrp**	Enable/disable the GVRP function for the switch.

10.2.3 Typical GVRP Application

Scenario:

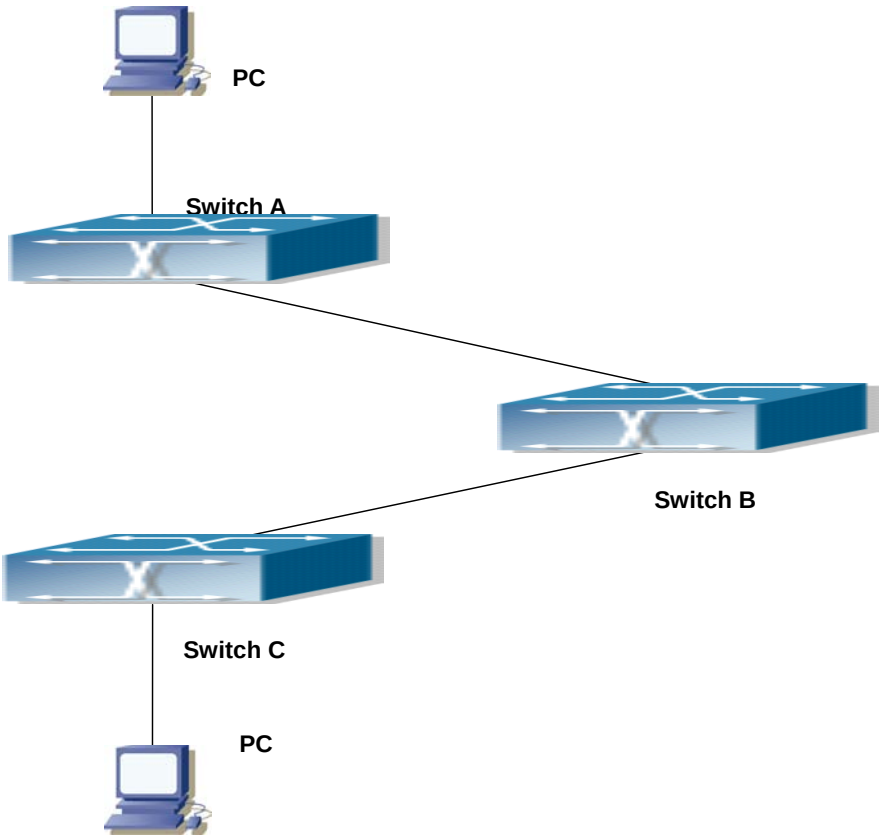


Figure 10-3 Typical GVRP Application Topology

To enable dynamic VLAN information register and update among switches, GVRP protocol is to be configured in the switch. Configure GVRP in Switch A, B and C, enable Switch B to learn VLAN100 dynamically so that the two workstation connected to VLAN100 in Switch A and C can communicate with each other through Switch B without static VLAN100 entries.

Configuration Item	Configuration description
VLAN100	Port 2 -6 of Switch A and C.
Trunk port	Port 11 of Switch A and C, Port 10, 11 of Switch B.
Global GVRP	Switch A, B, C.
Port GVRP	Port 11 of Switch A and C, Port 10, 11 of Switch B.

Connect the two workstation to the VLAN100 ports in switch A and B, connect port 11 of Switch A to port 10 of Switch B, and port 11 of Switch B to port 11 of Switch C.

The configuration steps are listed below:

Switch A:

```
Switch(config)# gvrp
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
```

```
Switch(Config-Vlan100)#exit
Switch(config)#interface Ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)# gvrp
Switch(Config-If-Ethernet1/11)#exit
```

Switch B:

```
Switch(config)# bridge-ext gvrp
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/10)# gvrp
Switch(Config-If-Ethernet1/10)#exit
Switch(config)#interface ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)# gvrp
Switch(Config-If-Ethernet1/11)#exit
```

Switch C:

```
Switch(config)# gvrp
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(config)#interface ethernet 1/11
Switch(Config-If-Ethernet1/11)#switchport mode trunk
Switch(Config-If-Ethernet1/11)# gvrp
Switch(Config-If-Ethernet1/11)#exit
```

10.2.4 GVRP Troubleshooting

The GARP counter setting in for Trunk ports in both ends of Trunk link must be the same, otherwise GVRP will not work properly. It is recommended to avoid enabling GVRP and RSTP at the same time in switch. If GVRP is to be enabled, RSTP function for the ports must be disabled first.

10.3 Dot1q-tunnel Configuration

10.3.1 Introduction to Dot1q-tunnel

Dot1q-tunnel is also called QinQ (802.1Q-in-802.1Q), which is an expansion of 802.1Q. Its dominating idea is encapsulating the customer VLAN tag (CVLAN tag) to the service provider VLAN tag (SPVLAN tag). Carrying the two VLAN tags the packet is transmitted through the backbone network of the ISP internet, so to provide a simple layer-2 tunnel for the users. It is simple and easy to manage, applicable only by static configuration, and especially adaptive to small office network or small scale metropolitan area network using layer-3 switch

as backbone equipment.

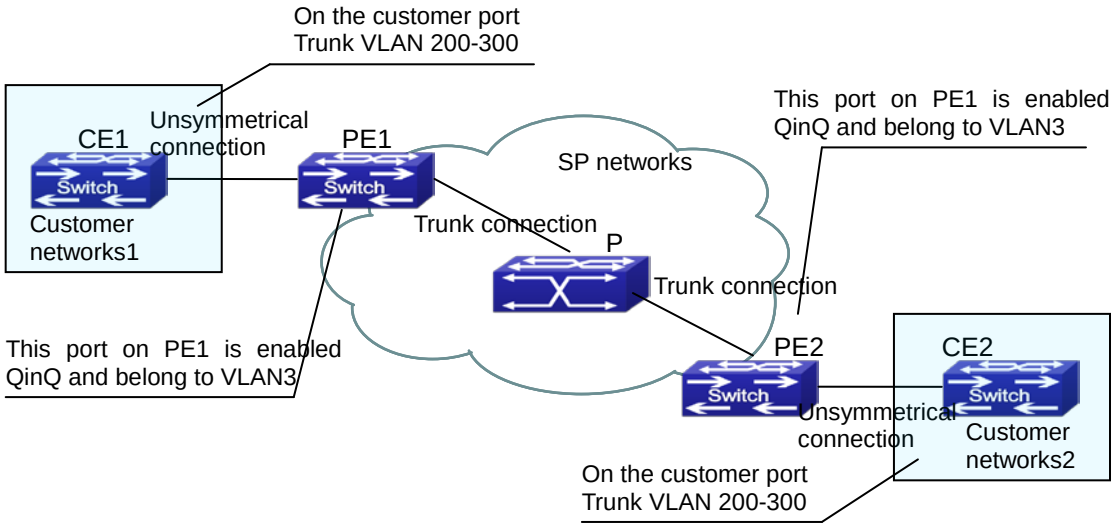


Figure 10-4 Dot1q-tunnel based Internetworking mode

As shown in above, after being enabled on the user port, dot1q-tunnel assigns each user an SPVLAN identification (SPVID). Here the identification of user is 3. Same SPVID should be assigned for the same network user on different PEs. When packet reaches PE1 from CE1, it carries the VLAN tag 200-300 of the user internal network. Since the dot1q-tunnel function is enabled, the user port on PE1 will add on the packet another VLAN tag, of which the ID is the SPVID assigned to the user. Afterwards, the packet will only be transmitted in VLAN3 when traveling in the ISP internet network while carrying two VLAN tags (the inner tag is added when entering PE1, and the outer is SPVID), whereas the VLAN information of the user network is open to the provider network. When the packet reaches PE2 and before being forwarded to CE2 from the client port on PE2, the outer VLAN tag is removed, then the packet CE2 receives is absolutely identical to the one sent by CE1. For the user, the role the operator network plays between PE1 and PE2, is to provide a reliable layer-2 link.

The technology of Dot1q-tuunel provides the ISP internet the ability of supporting many client VLANs by only one VLAN of theirselves. Both the ISP internet and the clients can configure their own VLAN independently.

It is obvious that, the dot1q-tunnel function has got following characteristics:

- Applicable through simple static configuration, no complex configuration or maintenance to be needed.
- Operators will only have to assign one SPVID for each user, which increases the number of concurrent supportable users; while the users has got the ultimate freedom in selecting and managing the VLAN IDs (select within 1~4094 at users' will).
- The user network is considerably independent. When the ISP internet is upgrading their network, the user networks do not have to change their original configuration.

Detailed description on the application and configuration of dot1q-tunnel will be provided in this section.

10.3.2 Dot1q-tunnel Configuration

Configuration Task Sequence of Dot1q-Tunnel:

1. Configure the dot1q-tunnel function on the ports
2. Configure the type of protocol (TPID) on the ports

1. Configure the dot1q-tunnel function on the ports

Command	Explanation
Port mode	
dot1q-tunnel enable **no dot1q-tunnel enable**	Enter/exit the dot1q-tunnel mode on the ports.

2. Configure the type of protocol (TPID) on the ports

Command	Explanation
Port mode	
dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1-65535>}	Configure the type of protocol on port.

10.3.3 Typical Applications of the Dot1q-tunnel

Scenario:

Edge switch PE1 and PE2 of the ISP internet forward the VLAN200~300 data between CE1 and CE2 of the client network with VLAN3. The port1 of PE1 is connected to CE1, port10 is connected to public network, the TPID of the connected equipment is 9100; port1 of PE2 is connected to CE2, port10 is connected to public network.

Configuration Item	Configuration Explanation
VLAN3	Port1 of PE1 and PE2.
dot1q-tunnel	Port1 of PE1 and PE2.
tpid	9100

Configuration procedure is as follows:

PE1:

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/1)# exit
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
switch(Config-Ethernet1/10)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/10)#exit
Switch(Config)#
```

PE2:

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/1)# exit
Switch(config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
switch(Config-Ethernet1/10)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/10)#exit
Switch(Config)#
```

10.3.4 Dot1q-tunnel Troubleshooting

- Enabling dot1q-tunnel on Trunk port will make the tag of the data packet unpredictable which is not required in the application. So it is not recommended to enable dot1q-tunnel on Trunk port .
- Configuring in port-channel is not supported.
- Enabled with STP/MSTP is not supported.
- Enabled with PVLAN is not supported.

10.4 Dynamic VLAN Configuration

10.4.1 Introduction to Dynamic VLAN

The dynamic VLAN is named corresponding to the static VLAN (namely the port based VLAN). Dynamic VLAN supported by the switch includes MAC-based VLAN, IP-subnet-based VLAN and Protocol-based VLAN. Detailed description is as follows:

The MAC-based VLAN division is based on the MAC address of each host, namely every host with a MAC address will be assigned to certain VLAN. By the means, the network user will maintain his membership in his belonging VLAN when moves from a physical location to another. As we can see the greatest advantage of this VLAN division is that the VLAN does not have to be re-configured when the user physic location change, namely shift from one switch to another, which is because it is user based, not switch port based.

The IP subnet based VLAN is divided according to the source IP address and its subnet mask of every host. It assigns corresponding VLAN ID to the data packet according to the subnet segment, leading the data packet to specified VLAN. Its advantage is the same as that of the MAC-based VLAN: the user does not have to change configuration when relocated.

The VLAN is divided by the network layer protocol, assigning different protocol to different VLANs. This is very attractive to the network administrators who wish to organize the user by applications and services. Moreover the user can move freely within the network while maintaining his membership. Advantage of this method enables user to change physical position without changing their VLAN residing configuration, while the VLAN can be divided by types of protocols which is important to the network administrators. Further, this method has

no need of added frame label to identify the VLAN which reduce the network traffic.

10.4.2 Dynamic VLAN Configuration

Dynamic VLAN Configuration Task Sequence:

1. Configure the MAC-based VLAN function on the port
2. Set the VLAN to MAC VLAN
3. Configure the correspondence between the MAC address and the VLAN
4. Configure the IP-subnet-based VLAN function on the port
5. Configure the correspondence between the IP subnet and the VLAN
6. Configure the correspondence between the Protocols and the VLAN
7. Adjust the priority of the dynamic VLAN

1. Configure the MAC-based VLAN function on the port

Command	Explanation
Port Mode	
switchport mac-vlan enable **no switchport mac-vlan enable**	Enable/disable the MAC-based VLAN function on the port.

2. Set the VLAN to MAC VLAN

Command	Explanation
Global Mode	
mac-vlan vlan <*vlan-id*> **no mac-vlan**	Configure the specified VLAN to MAC VLAN; the "**no mac-vlan**" command cancels the MAC VLAN configuration of this VLAN.

3. Configure the correspondence between the MAC address and the VLAN

Command	Explanation
Global Mode	
mac-vlan mac <*mac-addrss*> vlan <*vlan-id*> priority <*priority-id*> **no mac-vlan {mac <*mac-addrss*>|all}**	Add/delete the correspondence between the MAC address and the VLAN, namely specified MAC address join/leave specified VLAN.

4. Configure the IP-subnet-based VLAN function on the port

Command	Explanation
Port Mode	
switchport subnet-vlan enable **no switchport subnet-vlan enable**	Enable/disable the port IP-subnet-base VLAN function on the port.

5. Configure the correspondence between the IP subnet and the VLAN

Command	Explanation
Global Mode	
subnet-vlan ip-address <*ipv4-addrss*> mask <*subnet-mask*> vlan <*vlan-id*> priority <*priority-id*> **no subnet-vlan {ip-address <*ipv4-addrss*> mask <*subnet-mask*>|all}**	Add/delete the correspondence between the IP subnet and the VLAN, namely specified IP subnet joins/leaves specified VLAN.

6. Configure the correspondence between the Protocols and the VLAN

Command	Explanation
Global Mode	
protocol-vlan mode {ethernetii etype <*etype-id*>|llc {dsap <*dsap-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>} vlan <*vlan-id*> priority <*priority-id*> **no protocol-vlan {mode {ethernetii etype <*etype-id*>|llc {dsap <*dsap-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>}|all}**	Add/delete the correspondence between the Protocols and the VLAN, namely specified protocol joins/leaves specified VLAN.

7. Adjust the priority of the dynamic VLAN

Command	Explanation
Global Mode	
dynamic-vlan mac-vlan prefer **dynamic-vlan subnet-vlan prefer**	Configure the priority of the dynamic VLAN.

10.4.3 Typical Application of the Dynamic VLAN

Scenario:

In the office network Department A belongs to VLAN100. Several members of this department often have the need to move within the whole office network. It is also required to ensure the resource for other members of the department to access VLAN 100. Assume one of the members is M, the MAC address of his PC is 00-30-4f-11-22-33, and similar configurations are assigned to other members.

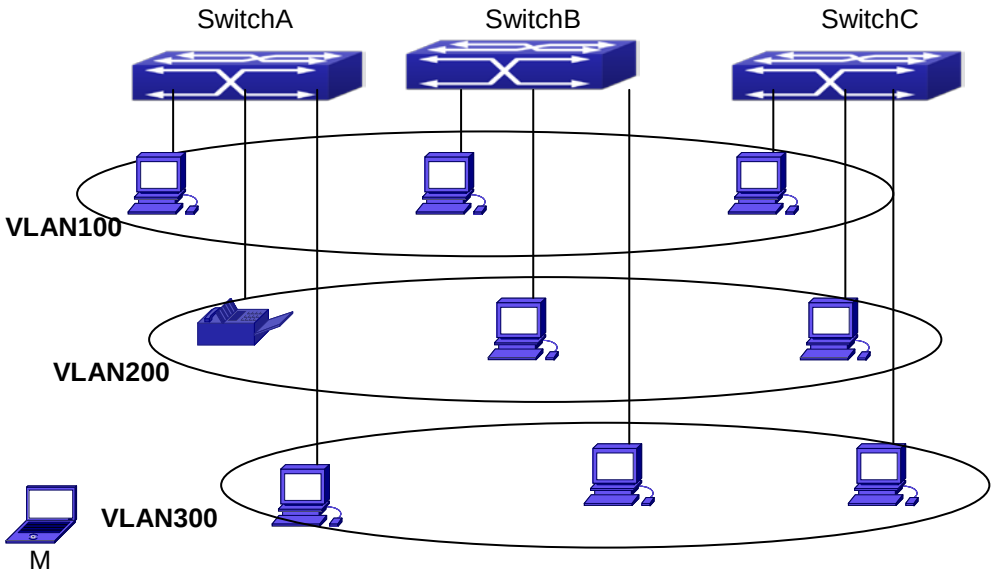


Figure 10-5 Typical topology application of dynamic VLAN

Configuration Items	Configuration Explanation
MAC-based VLAN	Global configuration on Switch A, Switch B, Switch C.

For example, M at E1/1 of SwitchA, then the configuration procedures are as follows:

Switch A, Switch B, Switch C:

```
switch(Config)#mac-vlan mac 00-30-4f-11-22-33 vlan 100 priority 0
switch(Config)#exit
switch#
```

10.4.4 Dynamic VLAN Troubleshooting

- On the switch configured with dynamic VLAN, if the two connected equipment (e.g. PC) are both belongs to the same dynamic VLAN, first communication between the two equipment may not go through. The solution will be letting the two equipment positively send data packet to the switch (such as ping), to let the switch learn their source MAC, then the two equipment will be able to communicate freely within the dynamic VLAN.

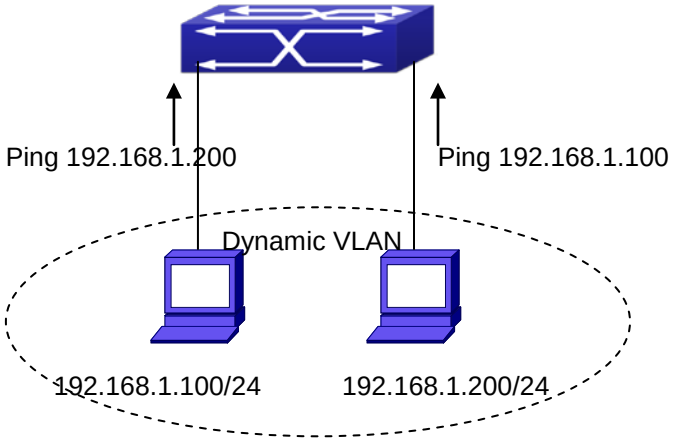


Figure 10-6 Dynamic VLAN Troubleshooting

10.5 Voice VLAN Configuration

10.5.1 Introduction to Voice VLAN

Voice VLAN is specially configured for the user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice equipments to the Voice VLAN, the user will be able to configure QoS (Quality of service) service for voice data, and improve the voice data traffic transmission priority to ensure the calling quality.

The switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment **OUI (Organizationally Unique Identifier)** will be considered the voice data traffic and transmitted to the Voice VLAN.

The configuration is based on MAC address, acquiring a mechanism in which every voice equipment transmitting information through the network has got its unique MAC address. VLAN will trace the address belongs to specified MAC. By This means, VLAN allows the voice equipment always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than switch port.

10.5.2 Voice VLAN Configuration

Voice VLAN Configuration Task Sequence:

1. Set the VLAN to Voice VLAN
2. Add a voice equipment to Voice VLAN
3. Enable the Voice VLAN on the port

1. Configure the VLAN to Voice VLAN

Command	Explanation
Global Mode	
voice-vlan vlan <*vlan-id*> **no voice-vlan**	Set/cancel the VLAN as a Voice VLAN

2. Add a Voice equipment to a Voice VLAN

Command	Explanation
Global Mode	
voice-vlan mac <*mac-address*> mask <*mac-mask*> priority <*priority-id*> [name <*voice-name*>] **no voice-vlan {mac <*mac-address*> mask <*mac-mask*>|name <*voice-name*> |all}**	Specify certain voice equipment join/leave the Voice VLAN

3. Enable the Voice VLAN of the port

Command	Explanation
Port Mode	
switchport voice-vlan enable **no switchport voice-vlan enable**	Enable/disable the Voice VLAN function on the port

10.5.3 Typical Applications of the Voice VLAN

Scenario:

A company realizes voice communication through configuring Voice VLAN. IP-phone1 and IP-phone2 can be connected to any port of the switch, namely normal communication and interconnected with other switches through the uplink port. IP-phone1 MAC address is 00-30-4f-11-22-33, connect port 1/1 of the switch, IP-phone2 MAC address is 00-30-4f-11-22-55, connect port 1/2 of the switch,.

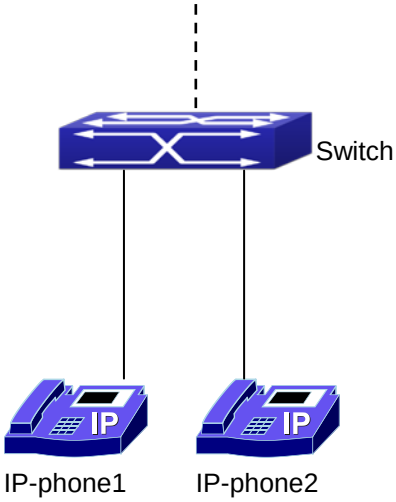


Figure 10-7 VLAN typical apply topology

Configuration items	Configuration Explanation
Voice VLAN	Global configuration on the Switch.

Configuration procedure:

Switch 1:

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#exit
Switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-30-4f-11-22-33 mask 255 priority 5 name company
Switch(config)#voice-vlan mac 00-30-4f-11-22-55 mask 255 priority 5 name company
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/10)#exit
```

10.5.4 Voice VLAN Troubleshooting

- Voice VLAN can not be applied concurrently with MAC-base VLAN
- The Voice VLAN support maximum 1024 sets of voice equipments, the exceeded number of equipments will not be supported
- The Voice VLAN on the port is enabled by default. If the configured data can no longer enter the Voice VLAN during operation, please check if the Voice VLAN function has been disabled on the port.

Chapter 11 MAC Table Configuration

11.1 Introduction to MAC Table

MAC table is a table identifies the mapping relationship between destination MAC addresses and switch ports. MAC addresses can be categorized as static MAC addresses and dynamic MAC addresses. Static MAC addresses are manually configured by the user, have the highest priority and are permanently effective (will not be overwritten by dynamic MAC addresses); dynamic MAC addresses are entries learnt by the switch in data frame forwarding, and is effective for a limited period. When the switch receives a data frame to be forwarded, it stores the source MAC address of the data frame and creates a mapping to the destination port. Then the MAC table is queried for the destination MAC address, if hit, the data frame is forwarded in the associated port, otherwise, the switch forwards the data frame to its broadcast domain. If a dynamic MAC address is not learnt from the data frames to be forwarded for a long time, the entry will be deleted from the switch MAC table.

There are two MAC table operations:

1. Obtain a MAC address.
2. Forward or filter data frame according to the MAC table.

11.1.1 Obtaining MAC Table

The MAC table can be built up statically and dynamically. Static configuration is to set up a mapping between the MAC addresses and the ports; dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

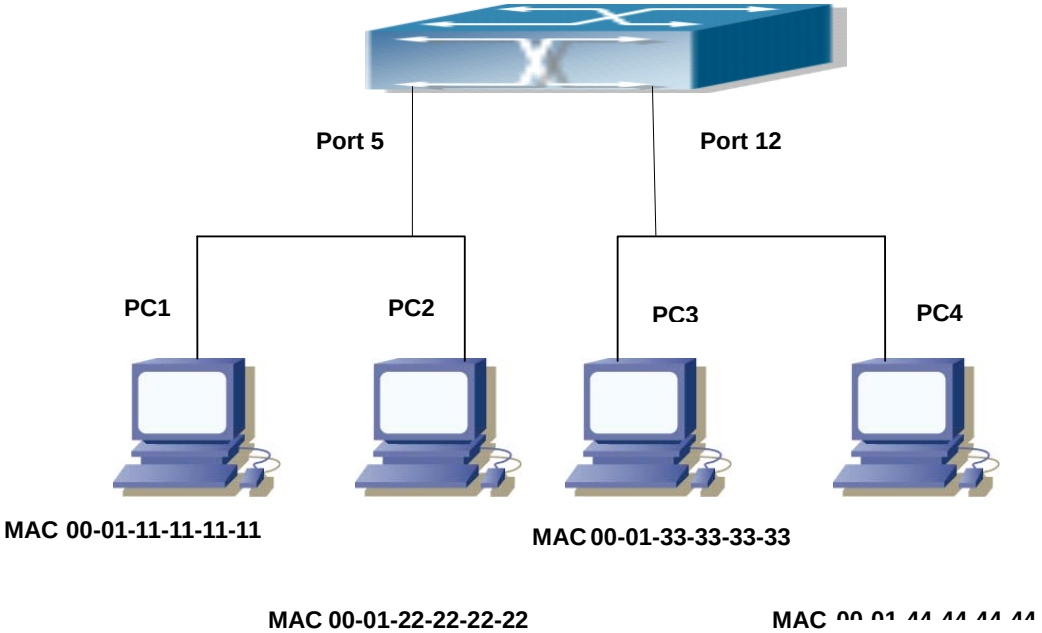


Figure 11-1 MAC Table dynamic learning

The topology of the figure above: 4 PCs connected to switch, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 1/5 of switch; PC3 and PC4 belongs to the same physical segment that connects to port 1/12 of switch.
The initial MAC table contains no address mapping entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process is as follow:

1. When PC1 sends message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 from this message, the mapping entry of 00-01-11-11-11-11 and port 1/5 is added to the switch MAC table.
2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port1/5, and no port mapping for 00-01-33-33-33-33 present, the switch broadcast this message to all the ports in the switch (assuming all ports belong to the default VLAN1).
3. PC3 and PC4 on port 1/12 receive the message sent by PC1, but PC4 will not reply, as the destination MAC address is 00-01-33-33-33-33, only PC3 will reply to PC1. When port 1/12 receives the message sent by PC3, a mapping entry for MAC address 00-01-33-33-33-33 and port 1/12 is added to the MAC table.
4. Now the MAC table has two dynamic entries, MAC address 00-01-11-11-11-11 - port 1/5 and 00-01-33-33-33-33 -port1/12.
5. After the communication between PC1 and PC3, the switch does not receive any message sent from PC1 and PC3. And the MAC address mapping entries in the MAC table are deleted after 300 seconds. The 300 seconds here is the default aging time for MAC address entry in switch. Aging time can be modified in switch.

11.1.2 Forward or Filter

The switch will forward or filter received data frames according to the MAC table. Take the above figure as an example, assuming switch have learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of switch will be:

MAC Address	Port number	Entry added by
00-01-11-11-11-11	1/5	Dynamic learning
00-01-22-22-22-22	1/5	Static configuration
00-01-33-33-33-33	1/12	Dynamic learning
00-01-44-44-44-44	1/12	Static configuration

1. Forward data according to the MAC table
   If PC1 sends a message to PC3, the switch will forward the data received on port 1/5 from port1/12.
2. Filter data according to the MAC table
   If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e. drop this message).

Three types of frames can be forwarded by the switch:

- Broadcast frame
- Multicast frame
- Unicast frame

The following describes how the switch deals with all the three types of frames:

- Broadcast frame: The switch can segregate collision domains but not broadcast domains. If no VLAN is set, all devices connected to the switch are in the same broadcast domain. When the switch receives a broadcast frame, it forwards the frame in all ports. When VLANs are configured in the switch, the MAC table will be adapted accordingly to add VLAN information. In this case, the switch will not forward the received broadcast frames in all ports, but forward the frames in all ports in the same VLAN.
- Multicast frame: When IGMP Snooping function is not enabled, multicast frames are processed in the same way as broadcast frames; when IGMP Snooping is enabled, the switch will only forward the multicast frames to the ports belonging to the very multicast group..
- Unicast frame: When no VLAN is configured, if the destination MAC addresses are in the switch MAC table, the switch will directly forward the frames to the associated ports; when the destination MAC address in a unicast frame is not found in the MAC table, the switch will broadcast the unicast frame. When VLANs are configured, the switch will forward unicast frame within the same VLAN. If the destination MAC address is found in the MAC table but belonging to different VLANs, the switch can only broadcast the unicast frame in the VLAN it belongs to.

11.2 Mac Address Table Configuration Task List

1. Configure the MAC address aging-time
2. Configure static MAC forwarding or filter entry

1. Configure the MAC aging-time

Command	Explanation
Global Mode	
mac-address-table aging-time *<0|aging-time>* **no mac-address-table aging-time**	Configure the MAC address aging-time.

2. Configure static MAC forwarding or filter entry

Command	Explanation
Global Mode	
mac-address-table {static | blackhole} address *<mac-addr>* vlan *<vlan-id >* [interface [ethernet | portchannel] *<interface-name>*] | [source|destination|both] **no mac-address-table {static | blackhole | dynamic} [address *<mac-addr>*] [vlan *<vlan-id>*] [interface [ethernet | portchannel] *<interface-name>*]**	Configure static MAC forwarding or filter entry.

11.3 Typical Configuration Examples

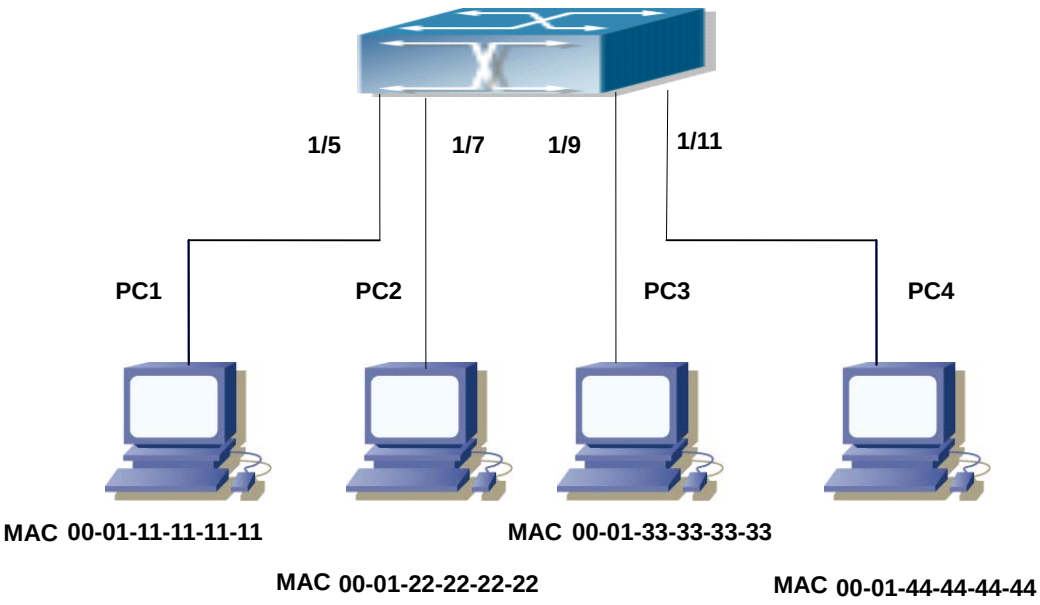


Figure 11-2 MAC Table typical configuration example

Scenario:

Four PCs as shown in the above figure connect to port 1/5、1/7、1/9、1/11 of switch, all the four PCs belong

to the default VLAN1. As required by the network environment, dynamic learning is enabled. PC1 holds sensitive data and can not be accessed by any other PC that is in another physical segment; PC2 and PC3 have static mapping set to port 7 and port 9, respectively.
The configuration steps are listed below:

1. Set the MAC address 00-01-11-11-11-11 of PC1 as a filter address.

```
Switch(config)#mac-address-table static 00-01-11-11-11-11 discard vlan 1.
```

2. Set the static mapping relationship for PC2 and PC3 to port 7 and port 9, respectively.

```
Switch(config)#mac-address-table static 00-01-22-22-22-22 interface ethernet 1/7 vlan 1
Switch(config)#mac-address-table static 00-01-33-33-33-33 interface ethernet 1/9 vlan 1
```

11.4 MAC Table Troubleshooting

Using the show mac-address-table command, a port is found to be failed to learn the MAC of a device connected to it. Possible reasons:

- The connected cable is broken.
- Spanning Tree is enabled and the port is in “discarding” status; or the device is just connected to the port and Spanning Tree is still under calculation, wait until the Spanning Tree calculation finishes, and the port will learn the MAC address.
- If not the problems mentioned above, please check for the switch portand contact technical support for solution.

11.5 MAC Address Function Extension

11.5.1 MAC Address Binding

11.5.1.1 Introduction to MAC Address Binding

Most switches support MAC address learning, each port can dynamically learn several MAC addresses, so that forwarding data streams between known MAC addresses within the ports can be achieved. If a MAC address is aged, the packet destined for that entry will be broadcasted. In other words, a MAC address learned in a port will be used for forwarding in that port, if the connection is changed to another port, the switch will learn the MAC address again to forward data in the new port.
However, in some cases, security or management policy may require MAC addresses to be bound with the ports, only data stream from the binding MAC are allowed to be forwarded in the ports. That is to say, after a MAC address is bound to a port, only the data stream destined for that MAC address can flow in from the binding port, data stream destined for the other MAC addresses that not bound to the port will not be allowed to pass through the port.

11.5.1.2 MAC Address Binding Configuration Task List

1. Enable MAC address binding function for the ports
2. Lock the MAC addresses for a port
3. MAC address binding property configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Port Mode	
switchport port-security **no switchport port-security**	Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no switchport port-security**" command disables the MAC address binding function for the port**,** and restores the MAC address learning function for the port.

2. Lock the MAC addresses for a port

Command	Explanation
Port Mode	
switchport port-security lock **no switchport port-security lock**	Lock the port, then MAC addresses learned will be disabled. The "**no switchport port-security lock**" command restores the function.
switchport port-security convert	Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses.
switchport port-security timeout <*value*> **no switchport port-security timeout**	Enable port locking timer function; the "**no switchport port-security timeout**" restores the default setting.
switchport port-security mac-address <*mac-address*> **no switchport port-security mac-address <*mac-address*>**	Add static secure MAC address; the "**no switchport port-security mac-address**" command deletes static secure MAC address.
Admin Mode	
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	Clear dynamic MAC addresses learned by the specified port.

3. MAC address binding property configuration

Command	Explanation
Port Mode	
switchport port-security maximum <*value*> **no switchport port-security maximum <*value*>**	Set the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the default value.
switchport port-security violation {protect | shutdown} **no switchport port-security violation**	Set the violation mode for the port; the "**no switchport port-security violation**" command restores the default setting.

11.5.1.3 Binding MAC Address Binding Troubleshooting

Enabling MAC address binding for ports may fail in some occasions. Here are some possible causes and solutions:

- If MAC address binding cannot be enabled for a port, make sure the port is not enabling port aggregation and is not configured as a Trunk port. MAC address binding is exclusive to such configurations. If MAC address binding is to be enabled, the functions mentioned above must be disabled first.
- If a secure address is set as static address and deleted, that secure address will be unusable even though it exists. For this reason, it is recommended to avoid static address for ports enabling MAC address.

Chapter 12 MSTP Configuration

12.1 Introduction to MSTP

The MSTP (Multiple STP) is a new spanning-tree protocol which is based on the STP and the RSTP. It runs on all the bridges of a bridged-LAN. It calculates a common and internal spanning tree (CIST) for the bridge-LAN which consists of the bridges running the MSTP, the RSTP and the STP. It also calculates the independent multiple spanning-tree instances (MSTI) for each MST domain (MSTP domain). The MSTP, which adopts the RSTP for its rapid convergence of the spanning tree, enables multiple VLANs to be mapped to the same spanning-tree instance which is independent to other spanning-tree instances. The MSTP provides multiple forwarding paths for data traffic and enables load balancing. Moreover, because multiple VLANs share a same MSTI, the MSTP can reduce the number of spanning-tree instances, which consumes less CPU resources and reduces the bandwidth consumption.

12.1.1 MSTP Region

Because multiple VLANs can be mapped to a single spanning tree instance, IEEE 802.1s committee raises the MST concept. The MST is used to make the association of a certain VLAN to a certain spanning tree instance.
A MSTP region is composed of one or multiple bridges with the same MCID (MST Configuration Identification) and the bridged-LAN (a certain bridge in the MSTP region is the designated bridge of the LAN, and the bridges attaching to the LAN are not running STP). All the bridges in the same MSTP region have the same MSID.

MSID consists of 3 attributes:

- Configuration Name: Composed by digits and letters
- Revision Level
- Configuration Digest: VLANs mapping to spanning tree instances

The bridges with the same 3 above attributes are considered as in the same MST region.
When the MSTP calculates CIST in a bridged-LAN, a MSTP region is considered as a bridge. See the figure below:

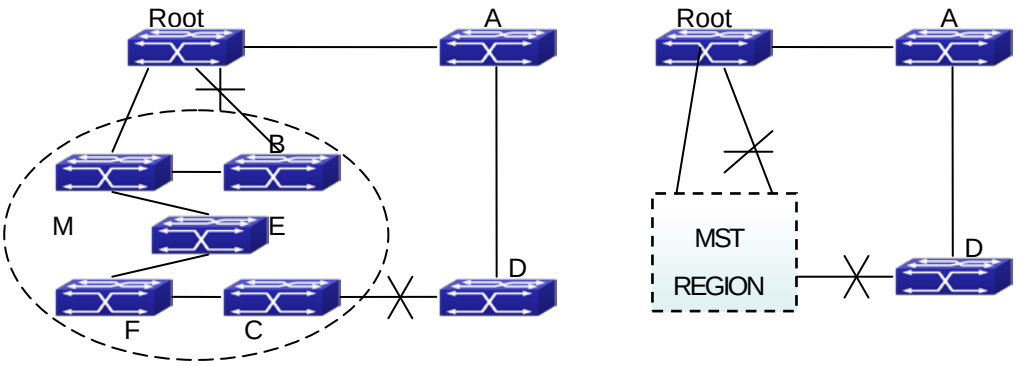


Figure 12-1 Example of CIST and MST Region

In the above network, if the bridges are running the STP or the RSTP, one port between Bridge M and Bridge B should be blocked. But if the bridges in the yellow range run the MSTP and are configured in the same MST region, MSTP will treat this region as a bridge. Therefore, one port between Bridge B and Root is blocked and one port on Bridge D is blocked.

12.1.1.1 Operations within an MSTP Region

The IST connects all the MSTP bridges in a region. When the IST converges, the root of the IST becomes the IST master, which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master is also the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP bridges at the boundary of the region is selected as the IST master.

When an MSTP bridge initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The bridge also initializes all of its MST instances and claims to be the root for all of them. If the bridge receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

Within a MST region, the IST is the only spanning-tree instance that sends and receives BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth.

12.1.1.2 Operations between MST Regions

If there are multiple regions or legacy 802.1D bridges within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP bridges in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The MSTI is only valid within its MST region. An MSTI has nothing to do with MSTIs in other MST regions. The bridges in a MST region receive the MST BPDU of other regions through Boundary Ports. They only process CIST related information and abandon MSTI information.

12.1.2 Port Roles

The MSTP bridge assigns a port role to each port which runs MSTP.

- CIST port roles: Root Port, Designated Port, Alternate Port and Backup Port
- On top of those roles, each MSTI port has one new role: Master Port.

The port roles in the CIST (Root Port, Designated Port, Alternate Port and Backup Port) are defined in the same ways as those in the RSTP.

12.1.3 MSTP Load Balance

In a MSTP region, VLANs can by mapped to various instances. That can form various topologies. Each instance is independent from the others and each distance can have its own attributes such as bridge priority and port cost etc. Consequently, the VLANs in different instances have their own paths. The traffic of the VLANs are load-balanced.

12.2 MSTP Configuration Task List

MSTP configuration task list:

1. Enable the MSTP and set the running mode
2. Configure instance parameters
3. Configure MSTP region parameters
4. Configure MSTP time parameters
5. Configure the fast migrate feature for MSTP
6. Configure the format of port packet
7. Configure the snooping attribute of authentication key
8. Configure the FLUSH mode once topology changes

1. Enable MSTP and set the running mode

Command	Explanation
Global Mode and Port Mode	
spanning-tree **no spanning-tree**	Enable/Disable MSTP.
Global Mode	
spanning-tree mode {mstp|stp|rstp} **no spanning-tree mode**	Set MSTP running mode.
Port Mode	
spanning-tree mcheck	Force port migrate to run under MSTP.

2. Configure instance parameters

Command	Explanation
Global Mode	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	Set bridge priority for specified instance.
spanning-tree priority <*bridge-priority*> **no spanning-tree priority**	Configure the spanning-tree priority of the switch.
Port Mode	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	Set port path cost for specified instance.
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*> port-priority**	Set port priority for specified instance.
spanning-tree mst <*instance-id*> rootguard **no spanning-tree mst <*instance-id*> rootguard**	Configure currently port whether running rootguard in specified instance, configure the rootguard port can't turn to root port.
spanning-tree *rootguard* **no spanning-tree *rootguard***	Configure currently port whether running rootguard in instance 0, configure the rootguard port can't turn to root port.

3. Configure MSTP region parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enter MSTP region mode. The no command restores the default setting.
MSTP region mode	
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	Create Instance and set mapping between VLAN and Instance.
name <*name*> **no name**	Set MSTP region name.
revision-level <*level*> **no revision-level**	Set MSTP region revision level.
abort	Quit MSTP region mode and return to Global mode without saving MSTP region configuration.
exit	Quit MSTP region mode and return to Global mode with saving MSTP region configuration.

4. Configure MSTP time parameters

Command	Explanation
Global Mode	
spanning-tree forward-time <time> **no spanning-tree forward-time**	Set the value for switch forward delay time.
spanning-tree hello-time <time> **no spanning-tree hello-time**	Set the Hello time for sending BPDU messages.
spanning-tree maxage <time> **no spanning-tree maxage**	Set Aging time for BPDU messages.
spanning-tree max-hop <hop-count> **no spanning-tree max-hop**	Set Maximum number of hops of BPDU messages in the MSTP region.

5. Configure the fast migrate feature for MSTP

Command	Explanation
Port Mode	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Set the port link type.
spanning-tree portfast [bpdufilter| bpduguard] **no spanning-tree portfast**	Set and cancel the port to be an boundary port. bpdufilter receives the BPDU discarding; bpduguard receives the BPDU will disable port; no parameter receives the BPDU, the port becomes a non-boundary port.

6. Configure the format of MSTP

Command	Explanation
Port Mode	
spanning-tree format standard **spanning-tree format privacy** **spanning-tree format auto** **no spanning-tree format**	Configure the format of port spanning-tree packet，standard format is provided by IEEE, privacy is compatible with CISCO and auto means the format is determined by checking the received packet.

7. Configure the snooping attribute of authentication key

Command	Explanation
Port Mode	
spanning-tree digest-snooping **no spanning-tree digest-snooping**	Set the port to use the authentication string of partner port. The no restores to use the generated string.

8. Configure the FLUSH mode once topology changes

Command	Explanation
Global Mode	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Enable: the spanning-tree flush once the topology changes. Disable: the spanning tree don't flush when the topology changes. Protect: the spanning-tree flush not more than one time every ten seconds. The no command restores to default setting, enable flush once the topology changes.
Port Mode	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Configure the port flush mode. The no command restores to use the global configured flush mode.

12.3 MSTP Example

The following is a typical MSTP application example:

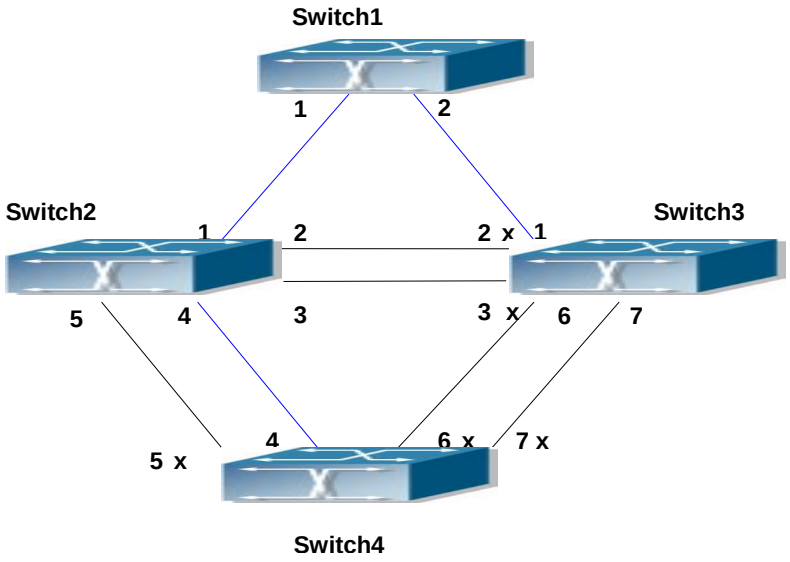


Figure 12-2 Typical MSTP Application Scenario

The connections among the switches are shown in the above figure. All the switches run in the MSTP mode by default, their bridge priority, port priority and port route cost are all in the default values (equal). The default configuration for switches is listed below:

Bridge Name		Switch1	Switch2	Switch3	Switch4
Bridge MAC Address		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Bridge Priority		32768	32768	32768	32768
Port Priority	Port 1	128	128	128	
	Port 2	128	128	128	
	Port 3		128	128	
	Port 4		128		128
	Port 5		128		128
	Port 6			128	128
	Port 7			128	128
Route Cost	Port 1	200000	200000	200000	
	Port 2	200000	200000	200000	
	Port 3		200000	200000	
	Port 4		200000		200000
	Port 5		200000		200000
	Port 6			200000	200000
	Port 7			200000	200000

By default, the MSTP establishes a tree topology (in blue lines) rooted with SwitchA. The ports marked with "x" are in the discarding status, and the other ports are in the forwarding status.

Configurations Steps:

Step 1: Configure port to VLAN mapping:

- Create VLAN 20, 30, 40, 50 in Switch2, Switch3 and Switch4.
- Set ports 1-7 as trunk ports in Switch2 Switch3 and Switch4.

Step 2: Set Switch2, Switch3 and Switch4 in the same MSTP:

- Set Switch2, Switch3 and Switch4 to have the same region name as mstp.
- Map VLAN 20 and VLAN 30 in Switch2, Switch3 and Switch4 to Instance 3; Map VLAN 40 and VLAN 50 in Switch2, Switch3 and Switch4 to Instance 4.

Step 3: Set Switch3 as the root bridge of Instance 3; Set Switch4 as the root bridge of Instance 4

- Set the bridge priority of Instance 3 in Switch3 as 0.
- Set the bridge priority of Instance 4 in Switch4 as 0.

The detailed configuration is listed below:

Switch2:

```
Switch2(config)#vlan 20
Switch2(Config-Vlan20)#exit
Switch2(config)#vlan 30
Switch2(Config-Vlan30)#exit
Switch2(config)#vlan 40
Switch2(Config-Vlan40)#exit
Switch2(config)#vlan 50
```

```
Switch2(Config-Vlan50)#exit
Switch2(config)#spanning-tree mst configuration
Switch2(Config-Mstp-Region)#name mstp
Switch2(Config-Mstp-Region)#instance 3 vlan 20;30
Switch2(Config-Mstp-Region)#instance 4 vlan 40;50
Switch2(Config-Mstp-Region)#exit
Switch2(config)#interface e1/1-7
Switch2(Config-Port-Range)#switchport mode trunk
Switch2(Config-Port-Range)#exit
Switch2(config)#spanning-tree
```

Switch3:

```
Switch3(config)#vlan 20
Switch3(Config-Vlan20)#exit
Switch3(config)#vlan 30
Switch3(Config-Vlan30)#exit
Switch3(config)#vlan 40
Switch3(Config-Vlan40)#exit
Switch3(config)#vlan 50
Switch3(Config-Vlan50)#exit
Switch3(config)#spanning-tree mst configuration
Switch3(Config-Mstp-Region)#name mstp
Switch3(Config-Mstp-Region)#instance 3 vlan 20;30
Switch3(Config-Mstp-Region)#instance 4 vlan 40;50
Switch3(Config-Mstp-Region)#exit
Switch3(config)#interface e1/1-7
Switch3(Config-Port-Range)#switchport mode trunk
Switch3(Config-Port-Range)#exit
Switch3(config)#spanning-tree
Switch3(config)#spanning-tree mst 3 priority 0
```

Switch4:

```
Switch4(config)#vlan 20
Switch4(Config-Vlan20)#exit
Switch4(config)#vlan 30
Switch4(Config-Vlan30)#exit
Switch4(config)#vlan 40
Switch4(Config-Vlan40)#exit
Switch4(config)#vlan 50
Switch4(Config-Vlan50)#exit
Switch4(config)#spanning-tree mst configuration
Switch4(Config-Mstp-Region)#name mstp
Switch4(Config-Mstp-Region)#instance 3 vlan 20;30
Switch4(Config-Mstp-Region)#instance 4 vlan 40;50
Switch4(Config-Mstp-Region)#exit
```

```
Switch4(config)#interface e1/1-7
Switch4(Config-Port-Range)#switchport mode trunk
Switch4(Config-Port-Range)#exit
Switch4(config)#spanning-tree
Switch4(config)#spanning-tree mst 4 priority 0
```

After the above configuration, Switch1 is the root bridge of the instance 0 of the entire network. In the MSTP region which Switch2, Switch3 and Switch4 belong to, Switch2 is the region root of the instance 0, Switch3 is the region root of the instance 3 and Switch4 is the region root of the instance 4. The traffic of VLAN 20 and VLAN 30 is sent through the topology of the instance 3. The traffic of VLAN 40 and VLAN 50 is sent through the topology of the instance 4. And the traffic of other VLANs is sent through the topology of the instance 0. The port 1 in Switch2 is the master port of the instance 3 and the instance 4.

The MSTP calculation generates 3 topologies: the instance 0, the instance 3 and the instance 4 (marked with blue lines). The ports with the mark “x” are in the status of discarding. The other ports are the status of forwarding. Because the instance 3 and the instance 4 are only valid in the MSTP region, the following figure only shows the topology of the MSTP region.

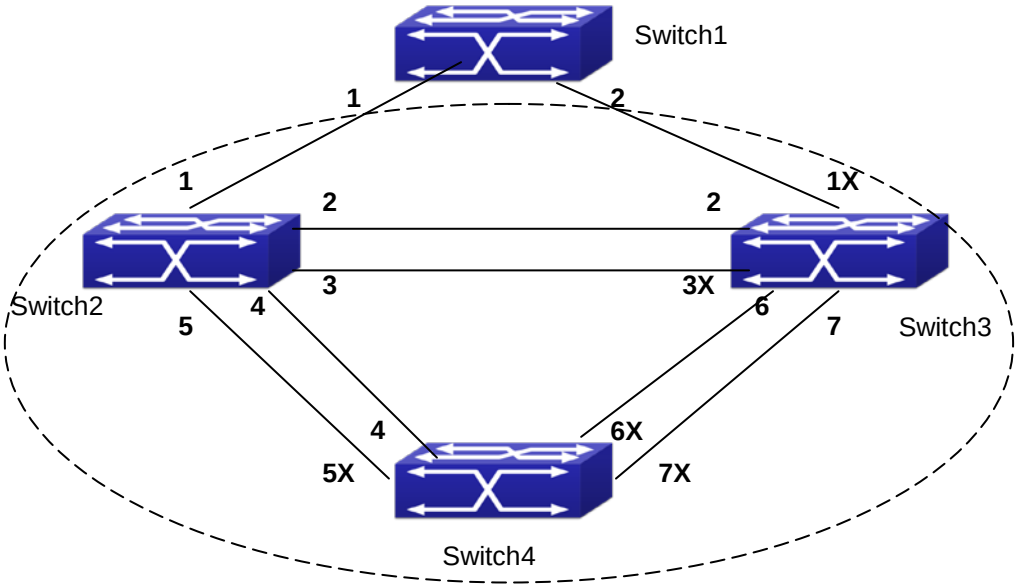


Figure 12-3 The Topology Of the Instance 0 after the MSTP Calculation

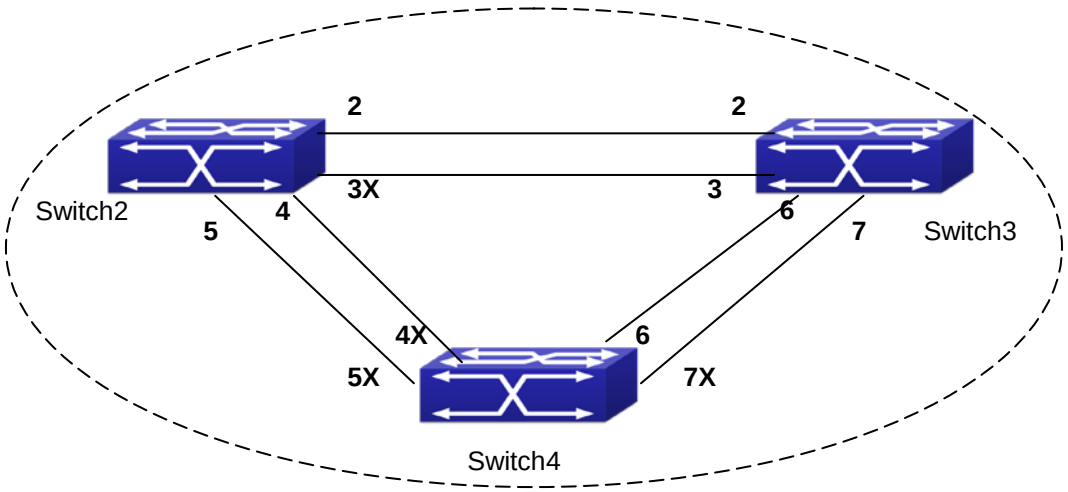


Figure 12-4 The Topology Of the Instance 3 after the MSTP Calculation

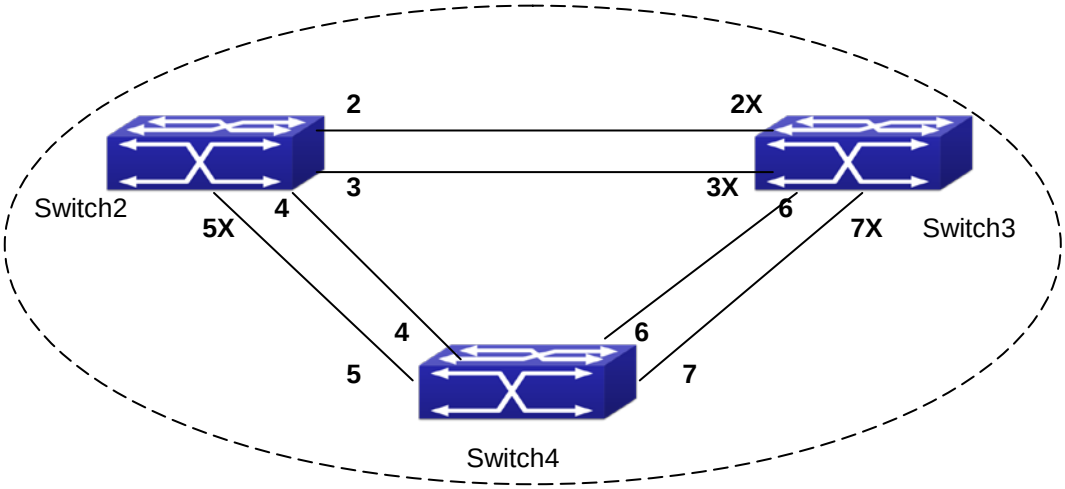


Figure 12-5 The Topology Of the Instance 4 after the MSTP Calculation

12.4 MSTP Troubleshooting

- In order to run the MSTP on the switch port, the MSTP has to be enabled globally. If the MSTP is not enabled globally, it can't be enabled on the port.
- The MSTP parameters co work with each other, so the parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

  2×(Bridge_Forward_Delay -1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- When users modify the MSTP parameters, they have to be sure about the changes of the topologies. The global configuration is based on the bridge. Other configurations are based on the individual instances.

Chapter 13 QoS Configuration

13.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

13.1.1 QoS Terms

QoS: Quality of Service, provides a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate new bandwidth but provides more effective bandwidth management according to the application requirement and network management.

QoS Domain: QoS Domain supports QoS devices to form a net-topology that provides Quality of Service, so this topology is defined as QoS Domain.

CoS: Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

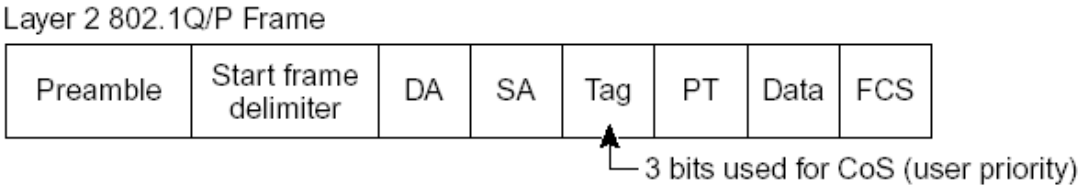


Figure 13-1 CoS priority

ToS: Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

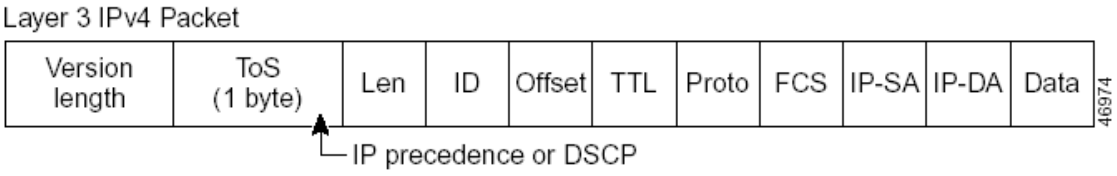
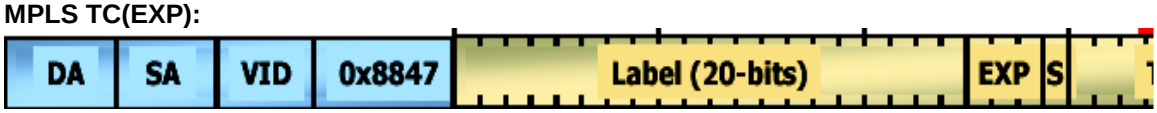


Figure 13-2 ToS priority

IP Precedence: IP priority. Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

MPLS TC(EXP):



A field of the MPLS packets means the service class, there are 3 bits, the ranging from 0 to 7.

Internal Priority: The internal priority setting of the switch chip, it's valid range relates with the chip, it's shortening is Int-Prio or IntP。

Drop Precedence: When processing the packets, firstly drop the packets with the bigger drop precedence, the ranging is 0-2 in three color algorithm, the ranging is 0-1 in dual color algorithm. It's shortening is Drop-Prec or DP.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark: Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Scheduling: QoS egress action. Configure the weight for eight egress queues WRR (Weighted Round Robin).

In-Profile: Traffic within the QoS policing policy range (bandwidth or burst value) is called "In-Profile".

Out-of-Profile: Traffic out the QoS policing policy range (bandwidth or burst value) is called "Out-of-Profile".

13.1.2 QoS Implementation

To implement the switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

13.1.3 Basic QoS Model

The basic QoS consists of four parts: Classification, Policing, Remark and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.

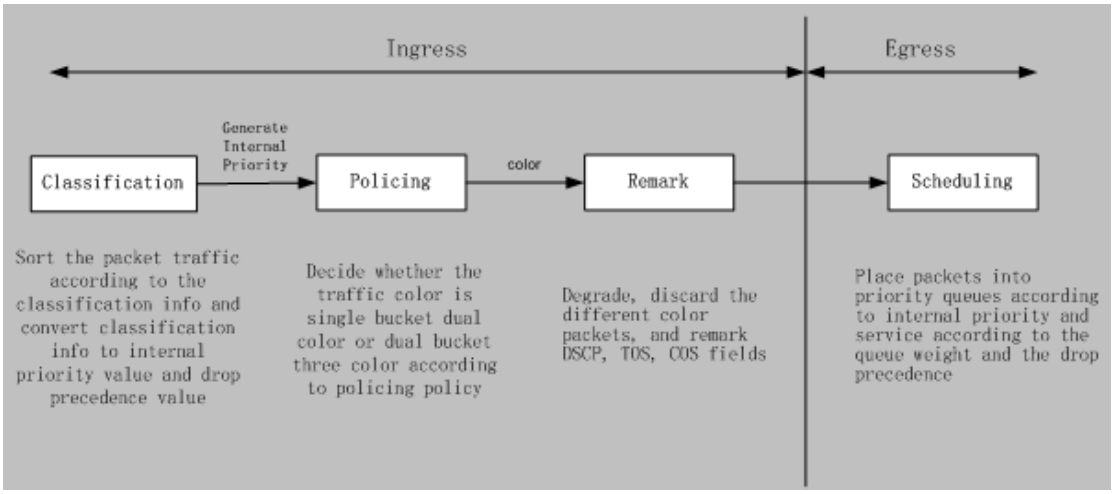


Figure 13-3 Basic QoS Model

Classification: Classify traffic according to packet classification information and generate internal priority and drop precedence based the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail.

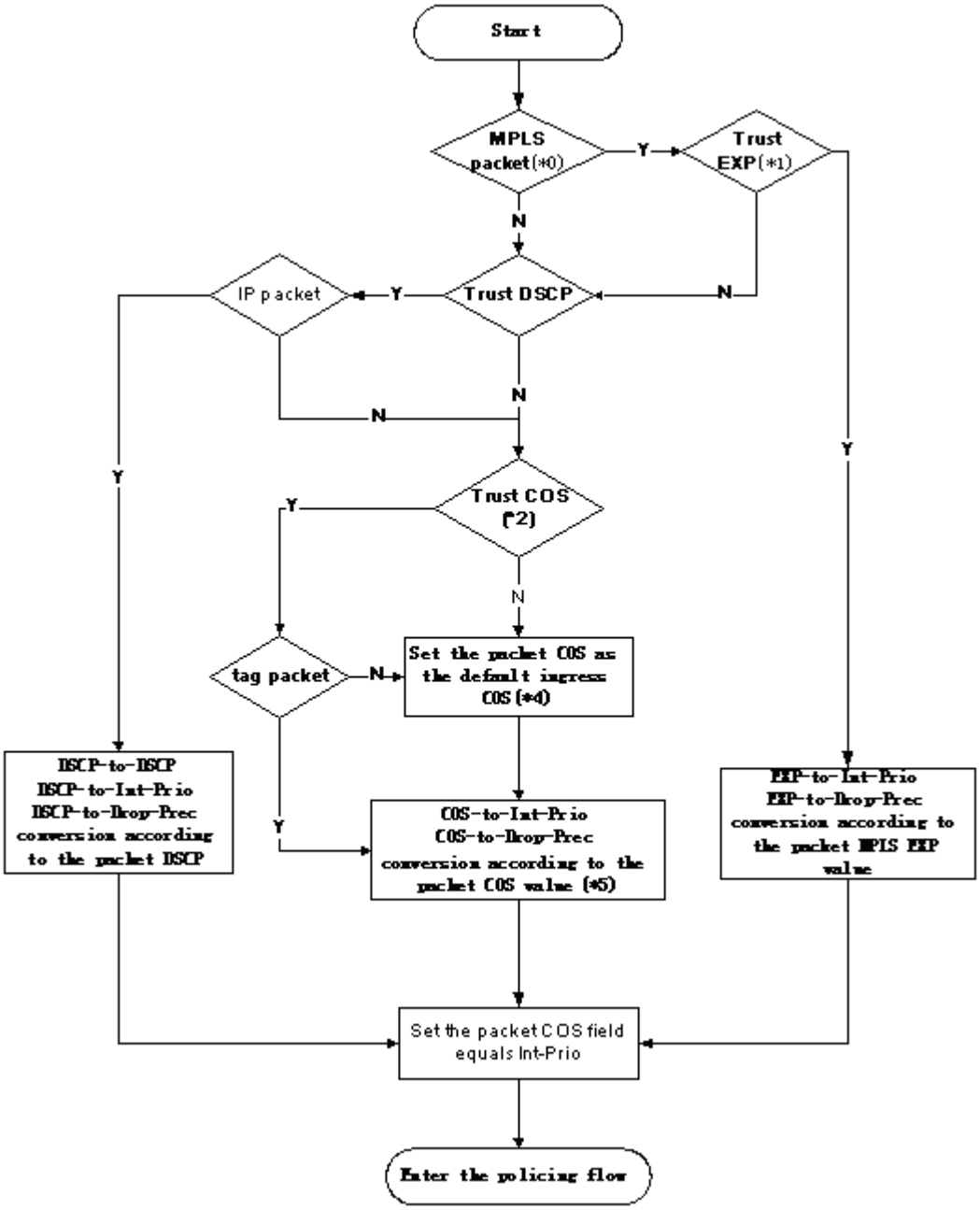


Figure 13-4 Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.

Policing can be performed based on the flow to configure different policies that allocate bandwidth to classified traffic, the assigned bandwidth policy may be dual bucket dual color or dual bucket three color. The traffic, will be assigned with different color, can be discarded or passed, for the passed packets, add the remarking action. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet.The following flowchart describes the operations.

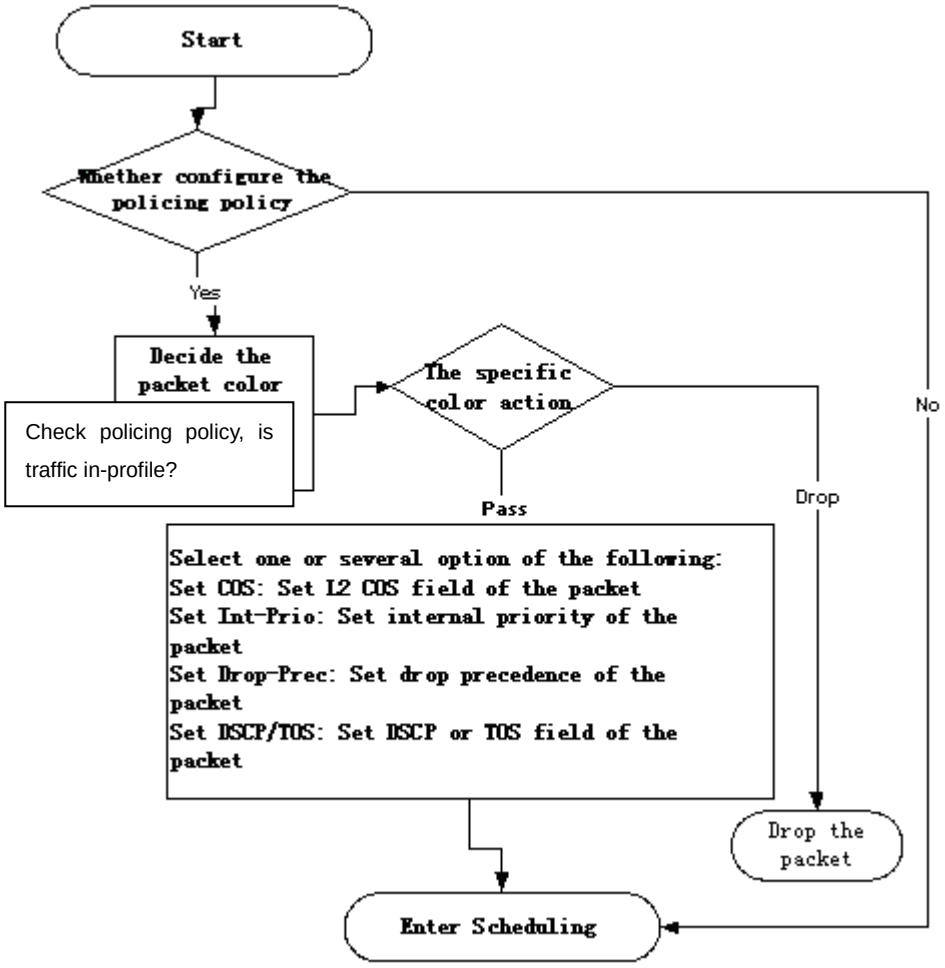


Figure 13-5 Policing and Remarking process

Queuing and scheduling: There are the internal priority and the drop precedence for the egress packets, the queuing operation assigns the packets to different priority queues according to the internal priority, while the scheduling operation perform the packet forwarding according to the priority queue weight and the drop precedence. The following flowchart describes the operations during queuing and scheduling.

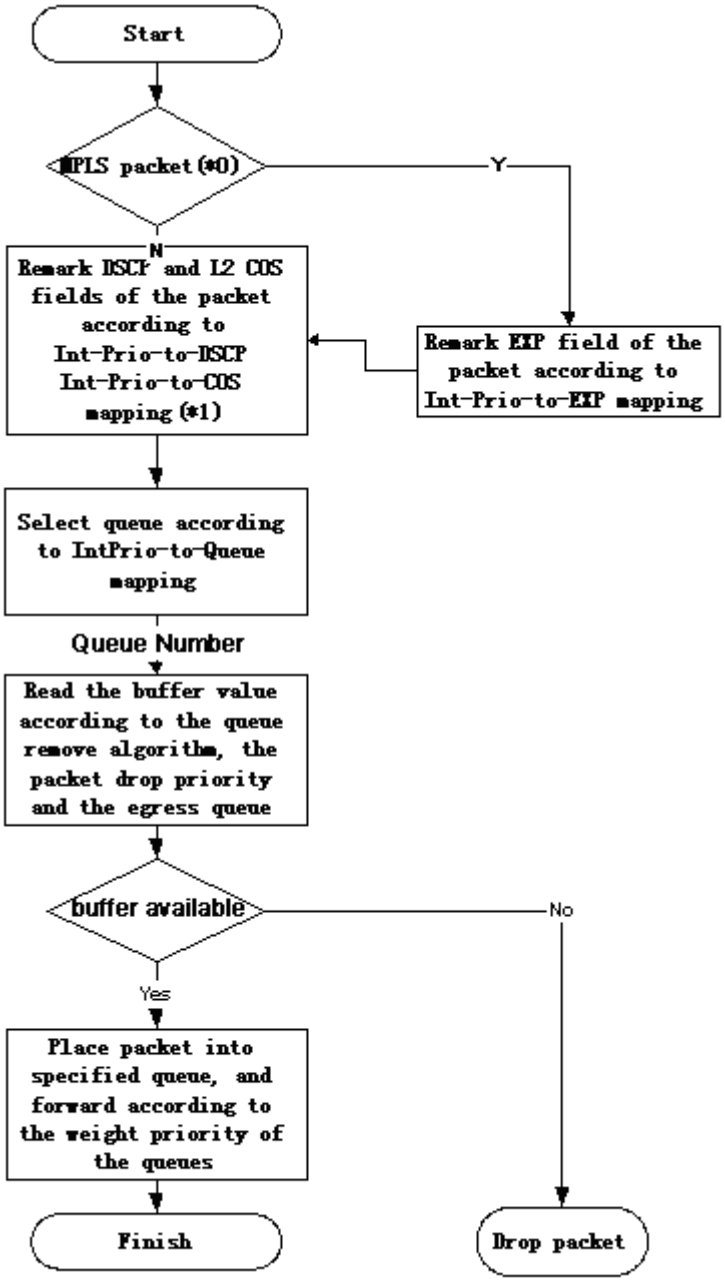


Figure 13-6 Queuing and Scheduling process

13.2 QoS Configuration Task List

1 · Configure class map.

Set up a classification rule according to ACL, CoS, VLAN ID, IPv4 Precedent, DSCP, IPV6 FL to classify the data stream. Different classes of data streams will be processed with different policies.

2 · Configure a policy map.

After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

3· Apply QoS to the ports or the VLAN interface

Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

The policy may be bound to the specific VLAN.

4· Configure queue management algorithm

Configure queue management algorithm, such as sp, wrr, wdrr, and so on.

5· Configure QoS mapping

Configure the mapping from CoS to DP, DSCP to DSCP, IntP or DP, IntP to DSCP.

1. Configure class map.

Command	Explanation
Global Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.
match {access-group <acl-index-or-name> | ip dscp <dscp-list> | ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <*cos-list*>} **no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos }**	Set matching criterion (classify data stream by ACL, CoS, VLAN ID, IPv4 Precedence, IPv6 FL or DSCP, etc) for the class map; the no command deletes specified matching criterion.

2. Configure a policy map

Command	Explanation
Global Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create a policy map and enter policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
class <*class-map-name*> [insert-before <class-map-name>] **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the no command deletes the specified class.
set {ip dscp <new-dscp> | ip precedence <new-precedence>|internal priority <new-inp>| drop precedence <new-dp> |cos <new-cos>}	Assign a new DSCP, CoS, IP Precedence value for the classified traffic; the no command cancels the newly assigned value.

no set {ip dscp | ip precedence|internal priority | drop precedence |cos }	
Single bucket mode: **policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION}| exceed-action ACTION})** **Dual bucket mode:** **policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }]** **ACTION definition:** **drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value>** **no policy**	Configure a policy for the classified flow. The non-aggregation policy command supports three colors. Analyze the working mode of the token bucket, whether it is singe rate single bucket, single rate dual bucket, dual rate dual bucket, set corresponding action to different color packets. The no command will delete the mode configuration. Single bucket mode is supported by the specific switch.
policy aggregate <*aggregate-policy-name*> **no policy aggregate <*aggregate-policy-name*>**	Apply a policy set to classified traffic; the no command deletes the specified policy set.
accounting **no accounting**	Set statistic function for the classified traffic. After enable this function under the policy class map mode, add statistic function to the traffic of the policy class map. In single bucket mode, the messages can only red or green when passing police. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of messages. In the print information, in-profile means green and out-profile means red and yellow.

3. Apply QoS to port or VLAN interface

Command	Explanation
Interface Configuration Mode	
mls qos trust {cos | dscp} **no mls qos trust {cos | dscp}**	Configure port trust; the no command disables the current trust status of the

	port.
mls qos cos {<*default-cos*>} **no mls qos cos**	Configure the default CoS value of the port; the no command restores the default setting.
service-policy input <*policy-map-name*> **no service-policy input <*policy-map-name*>**	Apply a policy map to the specified port; the no command deletes the specified policy map applied to the port. Egress policy map is not supported yet.
Global Mode	
service-policy input <*policy-map-name*> vlan <*vlan-list*> **no service-policy input <*policy-map-name*> vlan <*vlan-list*>**	Apply a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface.

4. Configure queue out method and weight

Command	Explanation
Interface Configuration Mode	
mls qos queue algorithm {sp | wrr | wdrr} **no mls qos queue algorithm**	Set queue management algorithm, the default queue management algorithm is wrr.
mls qos queue wrr weight <weight0..weight7> **no mls qos queue wrr weight**	Set queue weight based a port, the default queue weight is 1 2 3 4 5 6 7 8.
mls qos queue wdrr weight <weight0..weight7> **no mls qos queue wdrr weight**	Set queue weight based a port, the default queue weight is 10 20 40 80 160 320 640 1280.
mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> **no mls qos queue <queue-id> bandwidth**	Set bandwidth guarantee based a port.

5. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map (cos-dp <dp1…dp8> | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp>) **no mls qos map (cos-dp | dscp-dscp | dscp-intp | dscp-dp)**	Set the priority mapping for QoS, the no command restores the default mapping value.

mls qos map intp-dscp <dscp1..dscp8> **no mls qos map intp-dscp**	

6. Clear accounting data of the specific ports or VLANs

Command	Explanation
Interface Mode	
clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]	Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.

7. Show configuration of QoS.

Command	Explanation
Interface Mode	
show mls qos maps [cos-dp |dscp-dscp | dscp-intp | dscp-dp | intp-dscp]	Display the configuration of QoS mapping.
show class-map [<class-map-name>]	Display the classified map information of QoS.
show policy-map [<policy-map-name>]	Display the policy map information of QoS.
show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>}	Displays QoS configuration information on a port.

13.3 QoS Example

Example 1:
Enable QoS function, change the queue out weight of port ethernet 1/1 to 1:1:2:2:4:4:8:8, and set the port in trust QoS mode without changing DSCP value, and set the default QoS value of the port to 5.

The configuration steps are listed below:

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#wrr-queue bandwidth 1:1:2:2:4:4:8:8
Switch(Config-If-Ethernet1/1)#mls qos trust cos
Switch(Config-If-Ethernet1/1)#mls qos cos 5
```

Configuration result:
When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet1/1 is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through port ethernet1/1, it will be map to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8, respectively. If

the incoming packet has no CoS value, it is default to 5 and will be put in queue6. All passing packets would not have their DSCP values changed.

Example 2:

In port ethernet1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.

The configuration steps are listed below:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#service-policy input p1
```

Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet1/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Example 3:

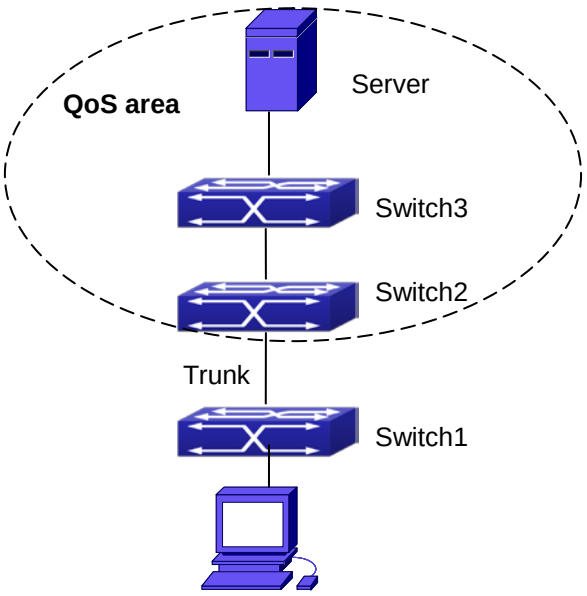


Figure 13-7 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, Switch1 classifies different traffics and assigns different IP precedences. For example, set CoS precedence for packets from segment 192.168.1.0 to 5 on port ethernet1/1. The port connecting to switch2 is a trunk port. In Switch2, set port ethernet 1/1 that connecting to swtich1 to trust CoS precedence. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below:

QoS configuration in SwitchA:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)# set ip precedence 5
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

QoS configuration in Switch2:

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos trust cos
```

13.4 QoS Troubleshooting

- trust cos and EXP can be used with other trust or Policy Map.
- trust dscp can be used with other trust or Policy Map. This configuration takes effect to IPv4 and IPv6 packets.
- trust exp, trust dscp and trust cos may be configured at the same time, the priority is: EXP>DSCP>COS.
- If the dynamic VLAN (mac vlan/voice vlan/ip subnet vlan/protocol vlan) is configured, then the packet COS value equals COS value of the dynamic VLAN.
- Policy map can only be bound to ingress direction, egress is not supported yet.
- At present, it is not recommended to use policy map on VLAN or VLAN's port.

Chapter 14 Flow-based Redirection

14.1 Introduction to Flow-based Redirection

Flow-based redirection function enables the switch to transmit the data frames meeting some special condition (specified by ACL) to another specified port. The fames meeting a same special condition are called a class of flow, the ingress port of the data frame is called the source port of redirection, and the specified egress port is called the destination port of redirection. Usually there are two kinds of application of flow-based redirection: 1. connecting a protocol analyzer (for example, Sniffer) or a RMON monitor to the destination port of redirection, to monitor and manage the network, and diagnose the problems in the network; 2. Special transmission policy for a special type of data frames.

The switch can only designate a single destination port of redirection for a same class of flow within a source port of redirection, while it can designate different destination ports of redirection for different classes of flows within a source port of redirection. The same class of flow can be applied to different source ports.

14.2 Flow-based Redirection Configuration Task Sequence

1． Flow-based redirection configuration

2． Check the current flow-based redirection configuration

1. Flow-based redirection configuration

Command	Explanation
Physical Interface Configuration Mode	
access-group <*aclname*> redirect to interface [ethernet <*IFNAME*>|<*IFNAME*>] **no access-group <*aclname*> redirect**	Specify flow-based redirection for the port; the "**no access-group <*aclname*> redirect**" command is used to delete flow-based redirection.

2. Check the current flow-based redirection configuration

Command	Explanation
Global Mode/Admin Mode	
show flow-based-redirect {interface [ethernet <*IFNAME*> |<*IFNAME*>]}	Display the information of current flow-based redirection in the system/port.

14.3 Flow-based Redirection Examples

Example:

User's request of configuration is listed as follows: redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6, that is sending the frames whose source IP is 192.168.1.111 received from port 1 through port6.

Modification of configuration:

1: Set an ACL, the condition to be matched is: source IP is 192.168.1.111;
2: Apply the redirection based on this flow to port 1.

The following is the configuration procedure:

```
Switch(config)#access-list 1 permit host 192.168.1.111
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6
```

14.4 Flow-based Redirection Troubleshooting Help

When the configuration of flow-based redirection fails, please check that whether it is the following reasons causing the problem:

- The type of flow (ACL) can only be digital standard IP ACL, digital extensive IP ACL, nomenclature standard IP ACL, nomenclature extensive IP ACL, digital standard IPv6 ACL, and nomenclature standard IPv6 ACL;
- Parameters of **Timerange** and **Portrange** can not be set in ACL, the type of ACL should be Permit.
- The redirection port must be 1000Mb port in the flow-based redirection function.

Chapter 15 Layer 3 Management Configuration

Switch only support Layer 2 forwarding, but can configure a Layer 3 management port for the communication of all kinds of management protocols based on the IP protocol.

15.1 Layer 3 Management Interface

15.1.1 Introduction to Layer 3 Management Interface

Only one layer 3 management interface can be created on switch. The Layer 3 interface is not a physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more layer 2 ports which belong to the same VLAN, or contain no layer 2 ports. At least one of the Layer 2 ports contained in Layer 3 interface should be in UP state for Layer 3 interface in UP state, otherwise, Layer 3 interface will be in DOWN state. The switch can use the IP addresses set in the layer 3 management interface to communicate with the other devices via IP.

15.1.2 Layer 3 Interface Configuration Task List

Layer 3 Interface Configuration Task List:

1. Create Layer 3 management interface

1. Create Layer 3 Management Interface

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Creates a management VLAN interface; the no command deletes the VLAN interface created in the switch.
ip default-gateway <ip-address> **no ip default-gateway <*ip-address*>**	Set the default-gateway address of switch; the no command will delete the default-gateway address.

15.2 IP Configuration

15.2.1 IP Configuration

Layer 3 interface can be configured as IPv4 interface, IPv6 interface.

15.2.1.1 IPv4 Address Configuration

IPv4 address configuration task list:
1 · Configure the IPv4 address of three-layer interface

1 · Configure the IPv4 address of three-layer interface

Command	Explanation
VLAN Interface Configuration Mode	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configure IP address of VLAN interface; the **no ip address [<*ip-address*> <*mask*>]** command cancels IP address of VLAN interface.

15.2.1.2 IPv6 Address Configuration

The configuration Task List of IPv6 is as follows:
1. IPv6 basic configuration
   (1) Configure interface IPv6 address
   (2) Configure default gateway

2. IPv6 Neighbor Discovery Configuration
   (1) Configure DAD neighbor solicitation message number
   (2) Configure send neighbor solicitation message interval
   (3) Enable and disable router advertisement
   (4) Configure router lifespan
   (5) Configure router advertisement minimum interval
   (6) Configure router advertisement maximum interval
   (7) Configure prefix advertisement parameters
   (8) Configure static IPv6 neighbor entries
   (9) Delete all entries in IPv6 neighbor table

1. IPv6 Basic Configuration
(1) Configure interface IPv6 address

Command	Explanation
Global mode	

ipv6 address ***<ipv6-address|prefix-length>*** **[eui-64]** **no ipv6 address** ***<ipv6-address/prefix-length>***	Configure IPv6 address, including aggregatable global unicast addresses, site-local addresses and link-local addresses. The **no ipv6 address** ***<ipv6-address/prefix-length>*** command cancels IPv6 address.

(2) Configure default gateway

Command	Explanation
Interface Configuration Mode	
ipv6 default-gateway <ipv6-address> **no ipv6 default-gateway <ipv6-address>**	Configure the default IPv6 gateway address; the no command deletes the default IPv6 gateway address.

2. IPv6 Neighbor Discovery Configuration

(1) Configure DAD Neighbor solicitation Message number

Command	Explanation
Interface Configuration Mode	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts**	Set the neighbor query message number sent in sequence when the interface makes duplicate address detection. The no command resumes default value (1).

(2) Configure Send Neighbor solicitation Message Interval

Command	Explanation
Interface Configuration Mode	
ipv6 nd ns-interval <*seconds*> **no ipv6 nd ns-interval**	Set the interval of the interface to send neighbor query message. The NO command resumes default value (1 second).

(3) Enable and disable router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd suppress-ra **no ipv6 nd suppress-ra**	Forbid IPv6 Router Advertisement. The NO command enables IPv6 router advertisement.

(4) Configure Router Lifespan

Command	Explanation
Interface Configuration Mode	

ipv6 nd ra-lifetime <seconds> **no ipv6 nd ra-lifetime**	Configure Router advertisement Lifespan. The NO command resumes default value (1800 seconds).

(5) Configure router advertisement Minimum Interval

Command	Description
Interface Configuration Mode	
ipv6 nd min-ra-interval <seconds> **no ipv6 nd min-ra-interval**	Configure the minimum interval for router advertisement. The NO command resumes default value (200 seconds).

(6) Configure router advertisement Maximum Interval

Command	**Explanation**
Interface Configuration Mode	
ipv6 nd max-ra-interval <seconds> **no ipv6 nd max-ra-interval**	Configure the maximum interval for router advertisement. The NO command resumes default value (600 seconds).

(7) Configure prefix advertisement parameters

Command	**Explanation**
Interface Configuration Mode	
ipv6 nd prefix **<ipv6-address/prefix-length>** ***<valid-lifetime>*** ***<preferred-lifetime>*** **[off-link]** **[no-autoconfig]** **no ipv6 nd prefix** ***<ipv6-address/prefix-length>*** ***<valid-lifetime>*** ***<preferred-lifetime>*** **[off-link]** **[no-autoconfig]**	Configure the address prefix and advertisement parameters of router. The NO command cancels the address prefix of routing advertisement.

(8) Configure static IPv6 neighbor Entries

Command	**Explanation**
Interface Configuration Mode	
ipv6 neighbor <ipv6-address> ***<hardware-address>*** **interface** ***<interface-type interface-number>***	Set static neighbor table entries, including neighbor IPv6 address, MAC address and two-layer port.
no ipv6 neighbor <ipv6-address>	Delete neighbor table entries.

(9) Delete all entries in IPv6 neighbor table

Command	Explanation
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries.

15.2.2 IPv6 Troubleshooting

- IPv6 on-off must be turned on when configuring IPv6 commands, otherwise the configuration is invalid
- If the connected PC has not obtained IPv6 address, you should check the RA announcement switch (the default is turned off)

15.3 ARP

15.3.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet MAC address. Switch supports static ARP configuration.

15.3.2 ARP Configuration Task List

ARP Configuration Task List:

1. Configure static ARP

1. Configure static ARP

Command	Explanation
VLAN Port Mode	
arp <*ip_address*> <*mac_address*> **no *arp* <ip_*address*>**	Configures a static ARP entry; the no command deletes a static ARP entry.

15.3.3 ARP Troubleshooting

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and create a solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP has not been learned, then enabled ARP debugging information and view the sending/receiving condition of ARP packets.
- Defective cable is a common cause of ARP problems and may disable ARP learning.

Chapter 16 ARP Scanning Prevention Function Configuration

16.1 Introduction to ARP Scanning Prevention Function

ARP scanning is a common method of network attack. In order to detect all the active hosts in a network segment, the attack source will broadcast lots of ARP messages in the segment, which will take up a large part of the bandwidth of the network. It might even do large-traffic-attack in the network via fake ARP messages to collapse of the network by exhausting the bandwidth. Usually ARP scanning is just a preface of other more dangerous attack methods, such as automatic virus infection or the ensuing port scanning, vulnerability scanning aiming at stealing information, distorted message attack, and DOS attack, etc.

Since ARP scanning threatens the security and stability of the network with great danger, so it is very significant to prevent it. Switch provides a complete resolution to prevent ARP scanning: if there is any host or port with ARP scanning features is found in the segment, the switch will cut off the attack source to ensure the security of the network.

There are two methods to prevent ARP scanning: port-based and IP-based. The port-based ARP scanning will count the number to ARP messages received from a port in a certain time range, if the number is larger than a preset threshold, this port will be “down”. The IP-based ARP scanning will count the number to ARP messages received from an IP in the segment in a certain time range, if the number is larger than a preset threshold, any traffic from this IP will be blocked, while the port related with this IP will not be “down”. These two methods can be enabled simultaneously. After a port or an IP is disabled, users can recover its state via automatic recovery function.

To improve the effect of the switch, users can configure trusted ports and IP, the ARP messages from which will not be checked by the switch. Thus the load of the switch can be effectively decreased.

16.2 ARP Scanning Prevention Configuration Task Sequence

1 · Enable the ARP Scanning Prevention function.
2 · Configure the threshold of the port-based and IP-based ARP Scanning Prevention
3 · Configure trusted ports
4 · Configure trusted IP
5 · Configure automatic recovery time
6 · Display relative information of debug information and ARP scanning

1. Enable the ARP Scanning Prevention function.

Command	Explanation
Global configuration mode	

anti-arpscan enable **no anti-arpscan enable**	Enable or disable the ARP Scanning Prevention function globally.

2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention

Command	Explanation
Global configuration mode	
anti-arpscan port-based threshold *<threshold-value>* **no anti-arpscan port-based threshold**	Set the threshold of the port-based ARP Scanning Prevention.
anti-arpscan ip-based threshold *<threshold-value>* **no anti-arpscan ip-based threshold**	Set the threshold of the IP-based ARP Scanning Prevention.

3. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-arpscan trust *<port* | *supertrust-port>* **no anti-arpscan trust *<port* | *supertrust-port>***	Set the trust attributes of the ports.

4. Configure trusted IP

Command	Explanation
Global configuration mode	
anti-arpscan trust ip *<ip-address>* [*<netmask>*] **no anti-arpscan trust ip *<ip-address>* [*<netmask>*]**	Set the trust attributes of IP.

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Enable or disable the automatic recovery function.
anti-arpscan recovery time *<seconds>* **no anti-arpscan recovery time**	Set automatic recovery time.

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	

anti-arpscan log enable **no anti-arpscan log enable**	Enable or disable the log function of ARP scanning prevention.
anti-arpscan trap enable **no anti-arpscan trap enable**	Enable or disable the SNMP Trap function of ARP scanning prevention.
show anti-arpscan [trust <*ip* | *port* | *supertrust-port*> | prohibited <*ip* | *port*>]	Display the state of operation and configuration of ARP scanning prevention.
Admin Mode	
debug anti-arpscan <*port* | *ip*> **no debug anti-arpscan <*port* | *ip*>**	Enable or disable the debug switch of ARP scanning prevention.

16.3 ARP Scanning Prevention Typical Examples

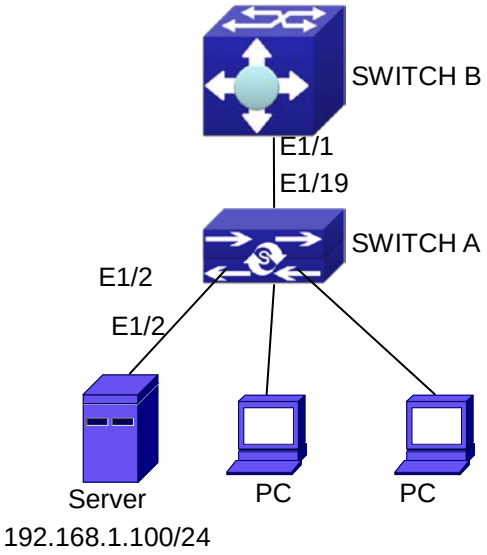


Figure 16-1 ARP scanning prevention typical configuration example

In the network topology above, port E1/1 of SWITCH B is connected to port E1/19 of SWITCH A, the port E1/2 of SWITCH A is connected to file server (IP address is 192.168.1.100), and all the other ports of SWITCH A are connected to common PC. The following configuration can prevent ARP scanning effectively without affecting the normal operation of the system.

SWITCH A configuration task sequence:

```
SwitchA(config)#anti-arpscan enable
SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
SwitchA(config)#interface ethernet1/2
SwitchA (Config-If-Ethernet1/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/2)#exit
SwitchA(config)#interface ethernet1/19
SwitchA (Config-If-Ethernet1/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/19)#exit
```

SWITCHB configuration task sequence:

```
Switch B(config)# anti-arpscan enable
SwitchB(config)#interface ethernet1/1
SwitchB (Config-If-Ethernet 1/1)#anti-arpscan trust port
SwitchB (Config-If-Ethernet 1/1)exit
```

16.4 ARP Scanning Prevention Troubleshooting Help

- ARP scanning prevention is disabled by default. After enabling ARP scanning prevention, users can enable the debug switch, "**debug anti-arpscan**", to view debug information.

Chapter 17 ARP GUARD Configuration

17.1 Introduction to ARP GUARD

There is serious security vulnerability in the design of ARP protocol, which is any network device, can send ARP messages to advertise the mapping relationship between IP address and MAC address. This provides a chance for ARP cheating. Attackers can send ARP REQUEST messages or ARP REPLY messages to advertise a wrong mapping relationship between IP address and MAC address, causing problems in network communication. The danger of ARP cheating has two forms: 1. PC4 sends an ARP message to advertise that the IP address of PC2 is mapped to the MAC address of PC4, which will cause all the IP messages to PC2 will be sent to PC4, thus PC4 will be able to monitor and capture the messages to PC2; 2. PC4 sends ARP messages to advertise that the IP address of PC2 is mapped to an illegal MAC address, which will prevent PC2 from receiving the messages to it. Particularly, if the attacker pretends to be the gateway and do ARP cheating, the whole network will be collapsed.

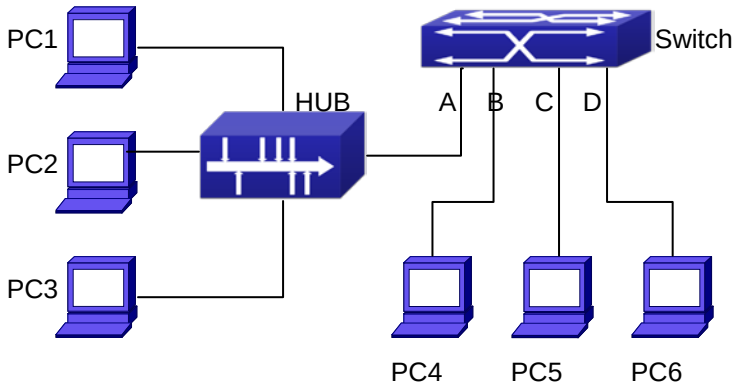


Figure 17-1 ARP GUARD schematic diagram

We utilize the filtering entries of the switch to protect the ARP entries of important network devices from being imitated by other devices. The basic theory of doing this is that utilizing the filtering entries of the switch to check all the ARP messages entering through the port, if the source address of the ARP message is protected, the messages will be directly dropped and will not be forwarded.

ARP GUARD function is usually used to protect the gateway from being attacked. If all the accessed PCs in the network should be protected from ARP cheating, then a large number of ARP GUARD address should be configured on the port, which will take up a big part of FFP entries in the chip, and as a result, might affect other applications. So this will be improper. It is recommended that adopting FREE RESOURCE related accessing scheme. Please refer to relative documents for details.

17.2 ARP GUARD Configuration Task List

1. Configure the protected IP address

Command	Explanation
Port configuration mode	
arp-guard ip <addr> **no arp-guard ip <addr>**	Configure/delete ARP GUARD address

Chapter 18 DHCP Configuration

18.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, and default route and host image file position within the network. DHCP is the enhanced version of BOOTP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of IP allocation and reduce user effort and cost on configuration. Another benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server. The implementation of DHCP is shown below:

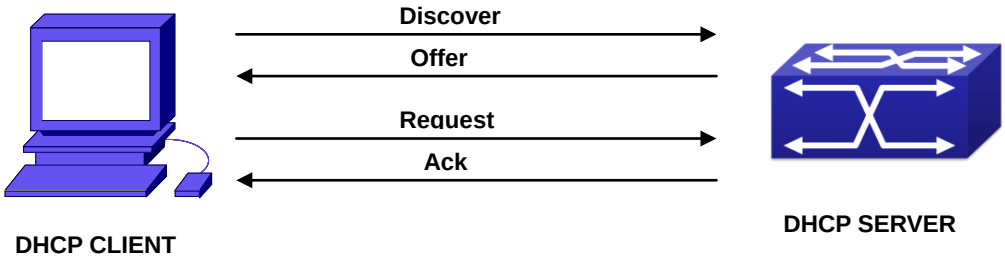


Figure 18-1 DHCP protocol interaction

Explanation:

1 · DHCP client broadcasts DHCPDISCOVER packets in the local subnet.

2 · On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.

3 · DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.

4 · The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will be sent to the client by the server. In this case, a DHCP relay is required to forward such DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

Switch can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are: 1) IP address obtained dynamically can be different every time;

manually bound IP address will be the same all the time. 2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless. 3) Dynamically allocated address cannot be bound manually. 4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

18.2 DHCP Server Configuration

DHCP Sever Configuration Task List:

1. Enable/Disable DHCP server
2. Configure DHCP Address pool
   (1) Create/Delete DHCP Address pool
   (2) Configure DHCP address pool parameters
   (3) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts

1. Enable/Disable DHCP server

Command	Explanation
Global Mode	
service dhcp **no service dhcp**	Enable DHCP server. The no command disables DHCP server.

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	Explanation
Global Mode	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configure DHCP Address pool. The no operation cancels the DHCP Address pool.

(2) Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> **[mask | prefix-length]** **no network-address**	Configure the address scope that can be allocated to the address pool. The no operation of this command cancels the allocation address pool.
default-router **[<*address1*>[<*address2*>[…<*address8*>]]]** **no default-router**	Configure default gateway for DHCP clients. The no operation cancels the default gateway.

dns-server [<*address1*>[<*address2*>[…<*address8*>]]] **no dns-server**	Configure DNS server for DHCP clients. The no command deletes DNS server configuration.
domain-name <*domain*> **no domain-name**	Configure Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [<*address1*>[<*address2*>[…<*address8*>]]] **no netbios-name-server**	Configure the address for WINS server. The no operation cancels the address for server.
netbios-node-type {b-node|h-node|m-node|p-node|<*type-number*>} **no netbios-node-type**	Configure node type for DHCP clients. The no operation cancels the node type for DHCP clients.
bootfile <*filename*> **no bootfile**	Configure the file to be imported for DHCP clients on boot up. The no command cancels this operation.
next-server [<*address1*>[<*address2*>[…<*address8*>]]] **no next-server [<*address1*>[<*address2*>[…<*address8*>]]]**	Configure the address of the server hosting file for importing. The no command deletes the address of the server hosting file for importing.
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configure the network parameter specified by the option code. The no command deletes the network parameter specified by the option code.
lease { days [hours][minutes] | infinite } **no lease**	Configure the lease period allocated to addresses in the address pool. The no command deletes the lease period allocated to addresses in the address pool.
Global Mode	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Exclude the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specify/delete the hardware address when assigning address manually.

host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specify/delete the IP address to be assigned to the specified client when binding address manually.
client-identifier <*unique-identifier*> **no client-identifier**	Specify/delete the unique ID of the user when binding address manually.

3. Enable logging for address conflicts

Command	Explanation
Global Mode	
ip dhcp conflict logging **no ip dhcp conflict logging**	Enable/disable logging for DHCP address to detect address conflicts.
Admin Mode	
clear ip dhcp conflict <*address* | all >	Delete a single address conflict record or all conflict records.

18.3 DHCP Configuration Examples

Scenario 1:

Too save configuration efforts of network administrators and users, a company is using switch as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WWW server	10.16.1.209
WINS node type	H-node		
Lease	3 days	Lease	1day

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as “management”.

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Switch(Config-Vlan-1)#exit
Switch(config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
```

```
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
Switch(config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Switch(config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab
Switch(dhcp-A1-config)#exit
```

Usage Guide: When a DHCP/BOOTP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.

If the DHCP/BOOTP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

18.4 DHCP Troubleshooting

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

- Verify the DHCP server is running, start the related DHCP server if not running.
- In such case, DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present, and (This does not indicate switch cannot assign IP address for different segments, see solution 2 for details.)
- In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command "**network-address**" and "**host**" are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

Chapter 19 DHCP Snooping Configuration

19.1 Introduction to DHCP Snooping

DHCP Snooping means that the switch monitors the IP-getting process of DHCP CLIENT via DHCP protocol. It prevents DHCP attacks and illegal DHCP SERVER by setting trust ports and untrust ports. And the DHCP messages from trust ports can be forwarded without being verified. In typical settings, trust ports are used to connect DHCP SERVER or DHCP RELAY Proxy, and untrust ports are used to connect DHCP CLINET. The switch will forward the DCHP request messages from untrust ports, but not DHCP reply ones. If any DHCP reply messages is received from a untrust port, besides giving an alarm, the switch will also implement designated actions on the port according to settings, such as “shutdown”, or distributing a “blackhole”. If DHCP Snooping binding is enabled, the switch will save binding information (including its MAC address, IP address, IP lease, VLAN number and port number) of each DHCP CLINET on untrust ports in DHCP snooping binding table With such information, DHCP Snooping can combine modules like dot1x and ARP, or implement user-access-control independently.

Defense against Fake DHCP Server: once the switch intercepts the DHCP Server reply packets（including DHCPOFFER, DHCPACK, and DHCPNAK）, it will alarm and respond according to the situation（shutdown the port or send Black hole）。

Defense against DHCP over load attacks: To avoid too many DHCP messages attacking CPU, users should limit the DHCP speed of receiving packets on trusted and non-trusted ports.

Record the binding data of DHCP: DHCP SNOOPING will record the binding data allocated by DHCP SERVER while forwarding DHCP messages, it can also upload the binding data to the specified server to backup it. The binding data is mainly used to configure the dynamic users of dot1x user based ports. Please refer to the chapter called“dot1x configuration” to find more about the usage of dot1x use-based mode.

Add binding ARP: DHCP SNOOPING can add static binding ARP according to the binding data after capturing binding data, thus to avoid ARP cheating.

Add trusted users: DHCP SNOOPING can add trusted user list entries according to the parameters in binding data after capturing binding data; thus these users can access all resources without DOT1X authentication.

Automatic Recovery: A while after the switch shut down the port or send blockhole, it should automatically recover the communication of the port or source MAC and send information to Log Server via syslog.

LOG Function: When the switch discovers abnormal received packets or automatically recovers, it should send syslog information to Log Server.

The Encryption of Private Messages: The communication between the switch and the inner network security management system TrustView uses private messages. And the users can encrypt those messages of version 2.

Add option82 Function: It is used with **dot1x dhcpoption82** authentication mode. Different option 82 will be

added in DHCP messages according to user's authentication status.

19.2 DHCP Snooping Configuration Task Sequence

1. Enable DHCP Snooping
2. Enable DHCP Snooping binding function
3. Enable DHCP Snooping binding ARP function
4. Enable DHCP Snooping option82 function
5. Set the private packet version
6. Set DES encrypted key for private packets
7. Set helper server address
8. Set trusted ports
9. Enable DHCP Snooping binding DOT1X function
10. Enable DHCP Snooping binding USER function
11. Adding static list entries function
12. Set defense actions
13. Set rate limitation of DHCP messages
14. Enable the debug switch

1· Enable DHCP Snooping

Command	Explanation
Globe mode	
ip dhcp snooping enable **no ip dhcp snooping enable**	Enable or disable the DHCP snooping function.

2· Enable DHCP Snooping binding

Command	Explanation
Globe mode	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Enable or disable the DHCP snooping binding function.

3· Enable DHCP Snooping binding ARP function

Command	Explanation
Globe mode	
ip dhcp snooping binding arp **no ip dhcp snooping binding arp**	Enable or disable the dhcp snooping binding ARP function.

4· Enable DHCP Snooping option82 function

Command	Explanation
Globe mode	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Enable/disable DHCP Snooping option 82 function.
ip dhcp snooping option82 enable **no ip dhcp snooping option82 enable**	To enable/delete DHCP option82 of dot1x in access switch.

5· Set the private packet version

Command	Explanation
Globe mode	
ip user private packet version two **no ip user private packet version two**	To configure/delete the private packet version.

6· Set DES encrypted key for private packets

Command	Explanation
Globe mode	
enable trustview key 0/7 <*password*> **no enable trustview key**	To configure/delete DES encrypted key for private packets.

7· Set helper server address

Command	Explanation
Globe mode	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) **no ip user helper-address (secondary|)**	Set or delete helper server address.

8· Set trusted ports

Command	Explanation
Port mode	
ip dhcp snooping trust **no ip dhcp snooping trust**	Set or delete the DHCP snooping trust attributes of ports.

9· Enable DHCP SNOOPING binding DOT1X function

Command	Explanation
Port mode	

ip dhcp snooping binding dot1x **no ip dhcp snooping binding dot1x**	Enable or disable the DHCP snooping binding dot1x function.

10 · Enable or disable the DHCP SNOOPING binding USER function

Command	Explanation
Port mode	
ip dhcp snooping binding user-control **no ip dhcp snooping binding user-control**	Enable or disable the DHCP snooping binding user function.

11 · Add static binding information

Command	Explanation
Globe mode	
ip dhcp snooping binding user <*mac*> address <*ipAddr*> <*mask*> vlan <*vid*> interface (ethernet|) <*ifname*> **no ip dhcp snooping binding user <*mac*> interface (ethernet|) <*ifname*>**	Add/delete DHCP snooping static binding list entries.

12 · Set defense actions

Command	Explanation
Port mode	
ip dhcp snooping action {shutdown|blackhole} [recovery <*second*>] **no ip dhcp snooping action**	Set or delete the DHCP snooping automatic defense actions of ports.

13 · Set rate limitation of data transmission

Command	Explanation
Globe mode	
ip dhcp snooping limit-rate <*pps*> **no ip dhcp snooping limit-rate**	Set rate limitation of the transmission of DHCP snooping messages.

14 · Enable the debug switch

Command	Explanation
Admin mode	

debug ip dhcp snooping packet **debug ip dhcp snooping event** **debug ip dhcp snooping update** **debug ip dhcp snooping binding**	Please refer to the chapter on system troubleshooting.

19.3 DHCP Snooping Typical Application

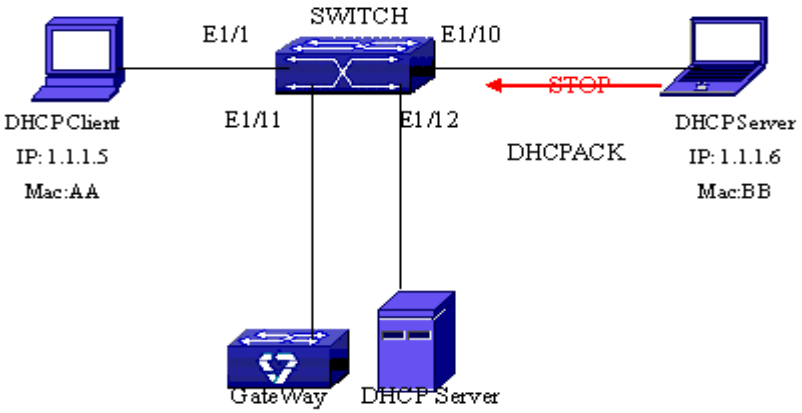


Figure 19-1 Sketch Map of TRUNK

As showed in the above chart, Mac-AA device is the normal user, connected to the non-trusted port 1/1 of the switch. It operates via DHCP Client, IP 1.1.1.5; DHCP Server and GateWay are connected to the trusted ports 1/11 and 1/12 of the switch; the malicious user Mac-BB is connected to the non-trusted port 1/10, trying to fake a DHCP Server（by sending DHCPACK）. Setting DHCP Snooping on the switch will effectively detect and block this kind of network attack.

Configuration sequence is:

```
switch#
switch#config
switch(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/11
switch(Config-If-Ethernet1/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/11)#exit
switch(config)#interface ethernet 1/12
switch(Config-If-Ethernet1/12)#ip dhcp snooping trust
switch(Config-If-Ethernet1/12)#exit
switch(config)#interface ethernet 1/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

19.4 DHCP Snooping Troubleshooting Help

19.4.1 Monitor and Debug Information

The “debug ip dhcp snooping” command can be used to monitor the debug information.

19.4.2 DHCP Snooping Troubleshooting Help

If there is any problem happens when using DHCP Snooping function, please check if the problem is caused by the following reasons:

- Check that whether the global DHCP Snooping is enabled;
- If the port does not react to invalid DHCP Server packets, please check that whether the port is set as a non-trusted port of DHCP Snooping.

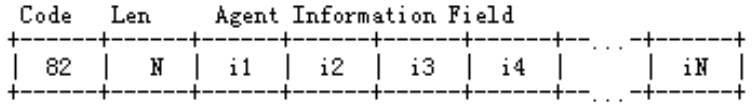
Chapter 20 DHCP Snooping option 82 Configuration

20.1 Introduction to DHCP Snooping option 82

DHCP option 82 is the Relay Agent Information Option, its option code is 82. DHCP option 82 is aimed at strengthening the security of DHCP servers and improving the IP address configuration policy. Switch obtain DHCP request packets(include DHCPDISCOVER, DHCPREQUEST, DHCPINFORM and DHCPRELEASE), DHCP SNOOPING is addesd to option 82 by request packets (including the client's physical access port, the access device ID and other information), to the DHCP request message from the client then forwards the message to DHCP server. When the DHCP server which supports the option 82 function receives the message, it will allocate an IP address and other configuration information for the client according to preconfigured policies and the option 82 information in the message. At the same time, DHCP server can identify all the possible DHCP attack messages according to the information in option 82 and defend against them. DHCP SNOOPING will peel the option 82 from the reply messages it receives, and forward the reply message to the specified port of the network access device. The application of DHCP option 82 is transparent for the client.

20.1.1 DHCP option 82 Message Structure

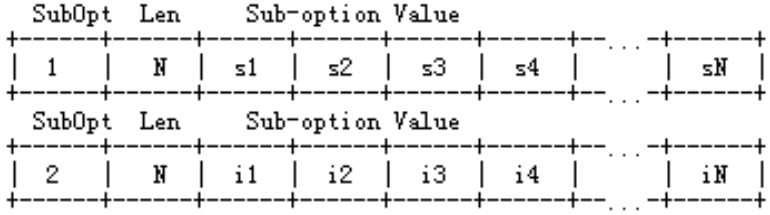
A DHCP message can have several option segments; option 82 is one of them. It has to be placed after other options but before option 255. The following is its format:



Code: represents the sequence number of the relay agent information option, the option 82 is called so because RFC3046 is defined as 82.

Len: the number of bytes in Agent Information Field, not including the two bytes in Code segment and Len segment.

Option 82 can have several sub-options, and need at least one sub-option. RFC3046 defines the following two sub-options, whose formats are showed as follows:



SubOpt: the sequence number of sub-option, the sequence number of Circuit ID sub-option is 1, the sequence number of Remote ID sub-option is 2.

Len: the number of bytes in Sub-option Value, not including the two bytes in SubOpt segment and Len segment.

20.1.2 option 82 Working Mechanism

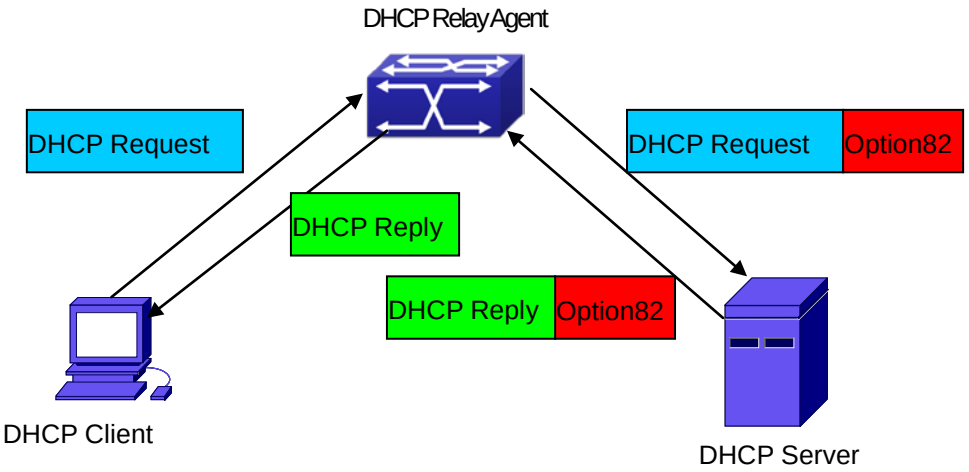


Figure 20-1 DHCP option 82 flow chart

If the DHCP SNOOPING supports option 82, the DHCP client should go through the following four steps to get its IP address from the DHCP server: discover, offer, select and acknowledge. The DHCP protocol follows the procedure below:

1）DHCP client sends a request broadcast message while initializing. This request message does not have option 82.

2）DHCP SNOOPING will add the option 82 to the end of the request message it receives, and perform layer 2 forwarding. By default, the sub-option 1 of option 82 (Circuit ID) is the interface information of the switch connected to the DHCP client (VLAN name and physical port name). The sub-option 2 of option 82(Remote ID) is the CPU MAC address of the switch.

3）After receiving the DHCP request message, the DHCP server will allocate IP address and other information for the client according to the information and preconfigured policy in the option segment of the message. Then it will forward the reply message with DHCP configuration information and option 82 information to DHCP SNOOPING.

4）DHCP SNOOPING will peel the option 82 information from the replay message sent by DHCP server, then the message with DHCP configuration information to perform layer 2 forwarding.

20.2 DHCP Snooping option 82 Configuration Task List

1． Enable DHCP SNOOPING
2． Enable DHCP Snooping binding function

3． Enable DHCP Snooping option 82 binding function

4． Configure trust ports

1. Enable DHCP SNOOPING

Command	**Explanation**
Global mode	
ip dhcp snooping enable **no ip dhcp snooping enable**	Enable or disable DHCP SNOOPING function.

2. Enable DHCP Snooping binding function

Command	**Explanation**
Interface configuration mode	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Enable or disable DHCP SNOOPING binding function.

3. Enable DHCP Snooping option 82 function

Command	Explanation
Global mode	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Enable or disable DHCP SNOOPING option 82 function.

4. Configure trust ports

Command	**Explanation**
Admin mode	
ip dhcp snooping trust **no ip dhcp snooping trust**	Set or delete DHCP SNOOPING trust attribute of ports.

20.3 DHCP option 82 Application Examples

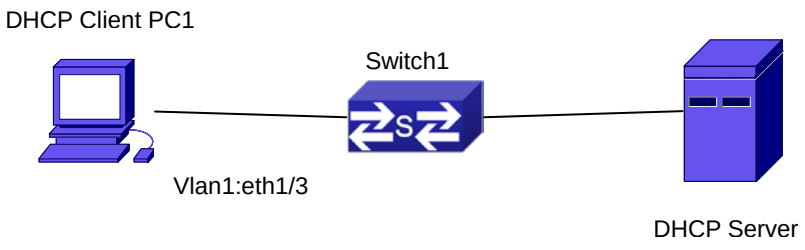


Figure 20-2 A DHCP option 82 typical application example

In the above example, layer 2 Switch1 will transmit the request message from DHCP client to DHCP serer through enable DHCP Snooping. It will also transmit the reply message from the server to DHCP client to finish the DHCP protocol procedure. After the DHCP SNOOPING option 82 function is enabled, the Switch1 appends the port information of accessing Switch1 to the request message from the client by option 82.

The following is the configuration of Switch1(MAC address is 00-30-4f-02-33-01):

```
Switch1(config)#ip dhcp snooping enable
Switch1(config)#ip dhcp snooping binding enable
Switch1(config)# ip dhcp snooping information enable
Switch1(Config-If-Ethernet1/12)#ip dhcp snooping trust
```

Linux ISC DHCP Server supports option 82, its configuration file /etc/dhcpd.conf is ddns-update-style interim;

```
ignore client-updates;

class "Switch1Vlan1Class1" {
match if option agent.circuit-id = "Vlan1+Ethernet1/3" and option agent.remote-id=00:03:0f:02:33:01;
}

subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch1Vlan1Class1";
}
}
```

Now, the DHCP server will allocate addresses for the network nodes from Switch1 within the range of 192.168.102.51 ~ 192.168.102.80.

20.4 DHCP Snooping option 82 Troubleshooting

- To implement the option 82 function of DHCP SNOOPING, the “debug ip dhcp snooping packet” command can be used during the operating procedure, including adding the option 82 information of the request message, the option 82 information peeled by the reply message.

Chapter 21 IPv4 Multicast Protocol

21.1 IPv4 Multicast Protocol Overview

This chapter will give an introduction to the configuration of IPv4 Multicast Protocol. All IPs in this chapter are IPv4.

21.1.1 Introduction to Multicast

Various transmission modes can be adopted when the destination of packet (including data, sound and video) transmission is the minority users in the network. One way is to use Unicast mode, i.e. to set up a separate data transmission path for each user; or, to use Broadcast mode, which is to send messages to all users in the network, and they will receive the Broadcast messages no matter they need or not. For example, if there are 200 users in a network who want to receive the same packet, then the traditional solution is to send this packet for 200 times separately via Unicast to guarantee the users who need the data can get all data wanted, or send the data in the entire domain via Broadcast. Transferring the data in the whole range of network .The users who need these data can get directly from the network. Both modes waste a great deal of valuable bandwidth resource, and furthermore, Broadcast mode goes against the security and secrecy.

The emergence of IP Multicast technology solved this problem in time. The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data packet, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to every user who needs it accurately and effectively.

It should be noticed that it is not necessary for Multicast source to join in Multicast group. It sends data to some Multicast groups, but it is not necessarily a receiver of the group itself. There can be more than one source sending packets to a Multicast group simultaneously. There may exist routers in the network which do not support Multicast, but a Multicast router can encapsulate the Multicast packets into Unicast IP packets with tunnel mode to send them to the Multicast router next to it, which will take off the Unicast IP header and continue the Multicast transmission process, thus a big alteration of network structure is avoided. The primary advantages of Multicast are:

1. Enhance efficiency: reduce network traffic, lighten the load of server and CPU
2. Optimize performance: reduce redundant traffic
3. Distributed application: Enable Multipoint Application

21.1.2 Multicast Address

The destination address of Multicast message uses class D IP address with range from 224.0.0.0 to 239.255.255.255. D class address can not appear in the source IP address field of an IP message. In the process of Unicast data transmission, the transmission path of a data packet is from source address routing to destination address, and the transmission is performed with hop-by-hop principle. However, in IP Multicast

environment, the destination addresses is a group instead of a single one, they form a group address. All message receivers will join in a group, and once they do, the data flowing to the group address will be sent to the receivers immediately and all members in the group will receive the data packets. The members in a Multicast group are dynamic, the hosts can join and leave the Multicast group at any time.

Multicast group can be permanent or temporary. Some of the Multicast group addresses are assigned officially; they are called Permanent Multicast Group. Permanent Multicast Group keeps its IP address fixed but its member structure can vary within. The member amount of Permanent Multicast Group can be arbitrary, even zero. The IP Multicast addresses which are not kept for use by Permanent Multicast Group can be utilized by temporary Multicast groups.

224.0.0.0～224.0.0.255 are reserved Multicast addresses (Permanent Group Address), address 224.0.0.0 is reserved but not assigned, and other addresses are used by Routing Protocol; 224.0.1.0～238.255.255.255 are Multicast addresses available to users（Temporary Group Address） and are valid in the entire domain of the network; 239.0.0.0～239.255.255.255 are local management Multicast addresses, which are valid only in specific local domain. Frequently used reserved multicast address list is as follows:

Benchmark address (reserved)
224.0.0.1 Address of all hosts
224.0.0.2 Address of all Multicast Routers
224.0.0.3 Unassigned
224.0.0.4 DVMRP Router
224.0.0.5 OSPF Router
224.0.0.6 OSPF DR
224.0.0.7 ST Router
224.0.0.8 ST host
224.0.0.9 RIP-2 Router
224.0.0.10 IGRP Router
224.0.0.11 Active Agent
224.0.0.12 DHCP Server/Relay Agent
224.0.0.13 All PIM Routers
224.0.0.14 RSVP Encapsulation
224.0.0.15 All CBT Routers
224.0.0.16 Specified SBM
224.0.0.17 All SBMS
224.0.0.18 VRRP
224.0.0.22 IGMP

When Ethernet transmits Unicast IP messages, the destination MAC address it uses is the receiver's MAC address. But in transmitting Multicast packets, the transmission destination is not a specific receiver any more, but a group with uncertain members, thus Multicast MAC address is used. Multicast MAC address is corresponding to Multicast IP address. It is prescribed in IANA (Internet Assigned Number Authority) that the higher 25 bits in Multicast MAC address is 0x01005e, and the lower 23bits in MAC address is the lower 23bits

in Multicast IP address.
Since only 23bits out of the lower 28bits in IP Multicast address are mapped into MAC address, therefore there are 32 IP Multicast addresses which are mapped into the same MAC address.

21.1.3 IP Multicast Packet Transmission

In Multicast mode, the source host sends packets to the host group indicated by the Multicast group address in the destination address field of IP data packet. Unlike Unicast mode, Multicast data packet must be forwarded to a number of external interfaces to be sent to all receiver sites in Multicast mode, thus Multicast transmission procedure is more complicated than Unicast transmission procedure.
In order to guarantee that all Multicast packets get to the router via the shortest path, the receipt interface of the Multicast packet must be checked in some certain way based on Unicast router table; this checking mechanism is the basis for most Multicast Routing Protocol to forward in Multicast mode --- RPF (Reverse Path Forwarding) check. Multicast router makes use of the impressed packet source address to query Unicast Router Table or independent Multicast Router Table to determine if the packet ingress interface is on the shortest path from receipt site to source address. If shortest path Tree is used, then the source address is the address of source host which sends Multicast Data Packets; if Shared Tree is used, then the source address is the address of the root of the Shared-Tree. When Multicast data packet gets to the router, if RPF check passes, then the data packet is forwarded according to Multicast forward item, and the data packet will be discarded else wise.

21.1.4 IP Multicast Application

IP Multicast technology has effectively solved the problem of sending in single point and receiving in multipoint. It has achieved the effective data transmission from a point to multiple points, saved a great deal of network bandwidth and reduced network load. Making use of the Multicast property of network, some new value-added operations can be supplied conveniently. In Information Service areas such as online living broadcast, network TV, remote education, remote medicine, real time video/audio meeting, the following applications may be supplied:

1) Application of Multimedia and Streaming Media
2) Data repository, finance application (stock) etc
3) Any data distribution application of “one point to multiple points”

In the situation of more and more multimedia operations in IP network, Multicast has tremendous market potential and Multicast operation will be generalized and popularized.

21.2 DCSCM

21.2.1 Introduction to DCSCM

DCSCM (Destination control and source control multicast) technology mainly includes three aspects, i.e. Multicast Packet Source Controllable, Multicast User Controllable and Service-Oriented Priority Strategy Multicast.

The Multicast Packet Source Controllable technology of Security Controllable Multicast technology is mainly processed in the following manners:

1· On the edge switch, if source under-control multicast is configured, then only multicast data from specified group of specified source can pass.

2· For RP switch in the core of PIM-SM, for REGISTER information out of specified source and specified group, REGISTER_STOP is transmitted directly and table entry is not allowed to set up. (This task is implemented in PIM-SM model).

The implement of Multicast User Controllable technology of Security Controllable Multicast technology is based on the control over IGMP report message sent out by the user, thus the model being controlled is IGMP snooping and IGMP model, of which the control logic includes the following three, i.e. to take control based on VLAN+MAC address transmitting packets, to take control based on IP address of transmitting packets and to take control based on the port where messages enter, in which IGMP snooping can use the above three methods to take control simultaneously, while since IGMP model is located at layer 3, it only takes control over the IP address transmitting packets .

The Service-Oriented Priority Strategy Multicast of Security Controllable technology adopts the following mode: for multicast data in limit range, set the priority specified by the user at the join-in end so that data can be sent in a higher priority on TRUNK port, consequently guarantee the transmission is processed in user-specified priority in the entire network.

21.2.2 DCSCM Configuration Task List

1. Source Control Configuration
2. Destination Control Configuration
3. Multicast Strategy Configuration

1· Source Control Configuration

Source Control Configuration has three parts, of which the first is to enable source control. The command of source control is as follows:

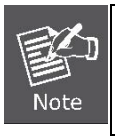
Command	Explanation
Global Configuration Mode	

[no] ip multicast source-control (Required)	Enable source control globally, the "**no ip multicast source-control**" command disables source control globally. It is noticeable that, after enabling source control globally, all multicast packets are discarded by default. All source control configuration can not be processed until that it is enabled globally, while source control can not be disabled until all configured rules are disabled.

he next is to configure the rule of source control. It is configured in the same manner as for ACL, and uses ACL number of 5000-5099, every rule number can be used to configure 10 rules. It is noticeable that these rules are ordered, the front one is the one which is configured the earliest. Once the configured rules are matched, the following rules won't take effect, so rules of globally allow must be put at the end. The commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] access-list <*5000-5099*> {deny|permit} ip {{<*source*> <*source-wildcard*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination*> <*destination-wildcard*>}|{host-destination <destination-host-ip>}|any-destination}	The rule used to configure source control. This rule does not take effect until it is applied to specified port. Using the NO form of it can delete specified rule.

The last is to configure the configured rule to specified port.



If the rules being configured will occupy the table entries of hardware, configuring too many rules will result in configuration failure caused by bottom table entries being full, so we suggest user to use the simplest rules if possible.

The configuration rules are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast source-control access-group <*5000-5099*>	Used to configure the rules source control uses to port, the NO form cancels the configuration.

2· Destination Control Configuration

Like source control configuration, destination control configuration also has three steps.

First, enable destination control globally. Since destination control need to prevent unauthorized user from

receiving multicast data, the switch won't broadcast the multicast data it received after configuring global destination control. Therefore, It should be avoided to connect two or more other Layer 3 switches in the same VLAN on a switch on which destination control is enabled. The configuration commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] multicast destination-control **（required）**	Globally enable destination control. The no operation of this command will globally disable destination control. All of the other configuration can only take effect after globally enabled. The next is configuring destination control rules, which are similar.

Next is to configure destination control rule. It is similar to source control, except to use ACL No. of 6000-7999.

Command	Explanation
Global Configuration Mode	
[no] access-list <*6000-7999*> {deny|permit} ip {{<*source*> <*source-wildcard*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination*> <*destination-wildcard*>}|{host-destination <*destination-host-ip*>}|any-destination}	The rule used to configure destination control. This rule does not take effect until it is applied to source IP or VLAN-MAC and port. Using the NO form of it can delete specified rule.

The last is to configure the rule to specified source IP, source VLAN MAC or specified port. It is noticeable that, due to the above situations, these rules can only be used globally in enabling IGMP-SNOOPING. And if IGMP-SNOOPING is not enabled, then only source IP rule can be used under IGMP Protocol. The configuration commands are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast destination-control access-group <*6000-7999*>	Used to configure the rules destination control uses to port, the NO form cancels the configuration.
Global Configuration Mode	
[no] ip multicast destination-control <*1-4094*> <*macaddr*> access-group <6000-7999>	Used to configure the rules destination control uses to specify VLAN-MAC, the NO form cancels the configuration.
[no] ip multicast destination-control <*IPADDRESS/M*> access-group <*6000-7999*>	Used to configure the rules destination control uses to specified IP address/net mask, the NO form cancels the configuration.

3． Multicast Strategy Configuration

Multicast Strategy uses the manner of specifying priority for specified multicast data to achieve and guarantee the effects the specific user requires. It is noticeable that multicast data can not get a special care all along unless the data are transmitted at TRUNK port. The configuration is very simple, it has only one command, i.e. to set priority for the specified multicast. The commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] ip multicast policy <*IPADDRESS/M*> <*IPADDRESS/M*> cos <*priority*>	Configure multicast strategy, specify priority for sources and groups in specific range, and the range is <0-7>.

21.2.3 DCSCM Configuration Examples

1． Source Control

In order to prevent an Edge Switch from putting out multicast data ad asbitsium, we configure Edge Switch so that only the switch at port Ethernet1/5 is allowed to transmit multicast, and the data group must be 225.1.2.3. Also, switch connected up to port Ethernet1/10 can transmit multicast data without any limit, and we can make the following configuration.

```
EC(config)#access-list 5000 permit ip any host 225.1.2.3
EC(config)#access-list 5001 permit ip any any
EC(config)#ip multicast source-control
EC(config)#interface ethernet1/5
EC(Config-If-Ethernet1/5)#ip multicast source-control access-group 5000
EC(config)#interface ethernet1/10
EC(Config-If-Ethernet1/10)#ip multicast source-control access-group 5001
```

2． Destination Control

We want to limit users with address in 10.0.0.0/8 network segment from entering the group of 238.0.0.0/8, so we can make the following configuration:

Firstly enable IGMP snooping in the VLAN it is located (Here it is assumed to be in VLAN2)

```
EC(config)#ip igmp snooping
EC(config)#ip igmp snooping vlan 2
```

After that, configure relative destination control access-list, and configure specified IP address to use that access-list.

```
Switch(config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
Switch(config)#access-list 6000 permit ip any any
```

```
Switch(config)#multicast destination-control
Switch(config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

In this way, users of this network segment can only join groups other than 238.0.0.0/8.

3· Multicast strategy

Server 210.1.1.1 is distributing important multicast data on group 239.1.2.3, we can configure on its join-in switch as follows:

```
Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4
```

In this way, the multicast stream will have a priority of value 4 (Usually this is pretty higher, the higher possible one is protocol data; if higher priority is set, when there is too many multicast data, it might cause abnormal behavior of the switch protocol) when it gets to other switches through this switch.

21.2.4 DCSCM Troubleshooting

The effect of DCSCM module itself is similar to ACL, and the problems occurred are usually related to improper configuration. Please read the descriptions above carefully. If you still can not determine the cause of the problem, please send your configurations and the effects you expect to the after-sale service staff of our company.

21.3 IGMP Snooping

21.3.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network device (such as a router) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send an IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with an IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

Switch provides IGMP Snooping and is able to send a query from the switch so that the user can use switch in IP multicast.

21.3.2 IGMP Snooping Configuration Task List

1. Enable IGMP Snooping
2. Configure IGMP Snooping

1. Enable IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping **no ip igmp snooping**	Enables IGMP Snooping. The no operation disables IGMP Snooping function.

2. Configure IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enables IGMP Snooping for specified VLAN. The no operation disables IGMP Snooping for specified VLAN.
ip igmp snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>} **no ip igmp snooping vlan < *vlan-id* > limit**	Configure the max group count of vlan and the max source count of every group. The "**no ip igmp snooping vlan <*vlan-id*> limit**" command cancels this configuration.
ip igmp snooping vlan <*vlan-id*> l2-general-querier **no ip igmp snooping vlan <*vlan-id*> l2-general-querier**	Set this vlan to layer 2 general querier. It is recommended to configure a layer 2 general querier on a segment. The "**no ip igmp snooping vlan <*vlan-id*> l2-general-querier**"command cancels this configuration.
ip igmp snooping vlan <vlan-id> l2-general-querier-version <version>	Configure the version number of a general query from a layer 2 general querier.
ip igmp snooping vlan <vlan-id> l2-general-querier-source <source>	Configure the source address of a general query from a layer 2 general querier.
ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Configure static mrouter port of vlan. The no form of the command cancels this configuration.
ip igmp snooping vlan <*vlan-id*> mrpt <*value* > **no ip igmp snooping vlan <*vlan-id*> mrpt**	Configure this survive time of mrouter port. The "**no ip igmp snooping vlan <*vlan-id*> mrpt**" command restores the default value.
ip igmp snooping vlan <*vlan-id*>	Configure this query interval. The "**no ip igmp**

query-interval <*value*> **no ip igmp snooping vlan <*vlan-id*> query-interval**	**snooping vlan <*vlan-id*> query-interval**" command restores the default value.
ip igmp snooping vlan <*vlan-id*> immediately-leave **no ip igmp snooping vlan <*vlan-id*> immediately-leave**	Enable the IGMP fast leave function for the specified VLAN: the "**no ip igmp snooping vlan <*vlan-id*> immediate-leave**" command disables the IGMP fast leave function.
ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*> **no ip igmp snooping vlan <*vlan-id*> query-mrsp**	Configure the maximum query response period. The "**no ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value.
ip igmp snooping vlan <vlan-id> query-robustness <*value*> **no ip igmp snooping vlan <vlan-id> query-robustness**	Configure the query robustness. The "**no ip igmp snooping vlan <vlan-id> query-robustness**" command restores to the default value.
ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*> **no ip igmp snooping vlan <*vlan-id*> suppression-query-time**	Configure the suppression query time. The "**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value.
ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*> **no ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*>**	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.
ip igmp snooping vlan <*vlan-id*> report source-address <*A.B.C.D*> **no ip igmp snooping vlan <*vlan-id*> report source-address**	Configure forwarding IGMP packet source address, the no operation cancels the packet source address.

21.3.3 IGMP Snooping Examples

Scenario 1: IGMP Snooping function

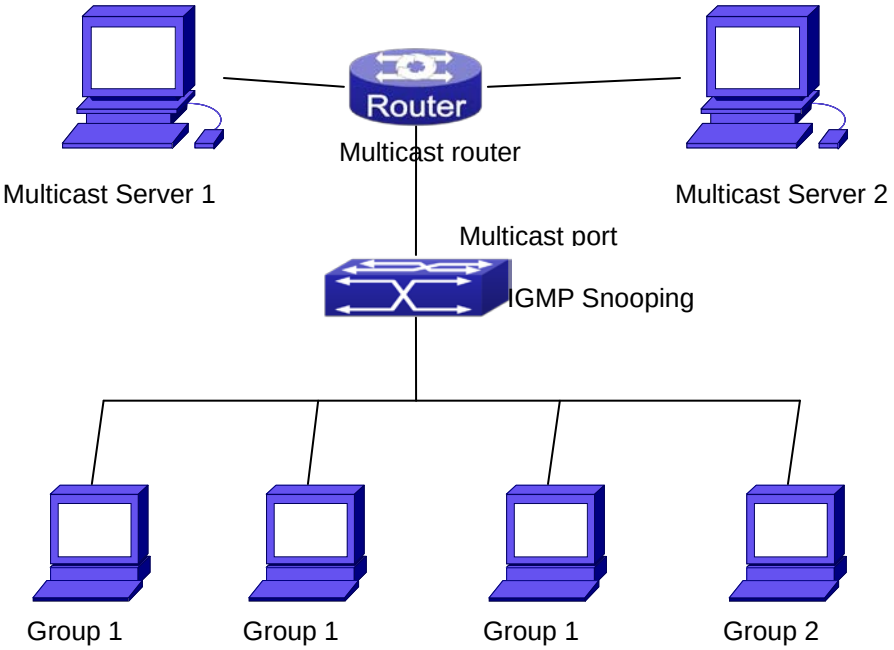


Figure 21-1 Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10, 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the mrouter port.

The configuration steps are listed below:

```
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 100
Switch(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1
```

Multicast Configuration

Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host is connected to port 12 plays program 2.

IGMP Snooping listening result:

The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group2.

All the four hosts can receive the program of their choice: ports 2, 6, 10 will not receive the traffic of program 2 and port 12 will not receive the traffic of program 1.

Scenario 2: L2-general-querier

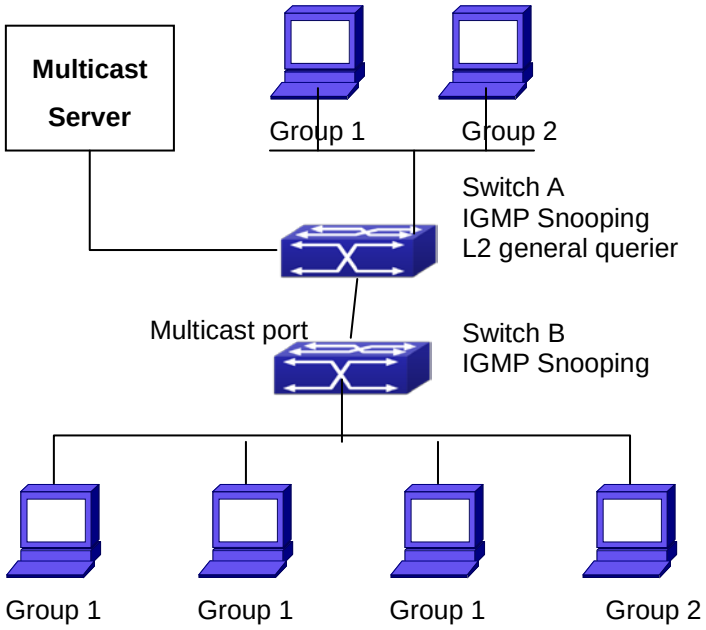


Figure 21-2 The switches as IGMP Queries

The configuration of Switch2 is the same as the switch in scenario 1, SwitchA takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in SwitchA, including ports 1, 2, 6, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

The configuration steps are listed below:

```
SwitchA#config
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 60
SwitchA(config)#ip igmp snooping vlan 60 L2-general-querier

SwitchB#config
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 100
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1
```

Multicast Configuration

The same as scenario 1

IGMP Snooping listening result:

Similar to scenario 1

Scenario 3: To run in cooperation with layer 3 multicast protocols.

SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure

PIM-SM on ROUTER, and enable PIM-SM on vlan 100 (use the same PIM mode with the connected multicast router)

Configurations are listed as below:

```
switch#config
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ip pim sparse-mode
```

IGMP snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

- Remove the layer 2 multicast entries.
- Provide query functions to the layer 3 with vlan, S, and G as the parameters.
- When layer 3 IGMP is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IPMC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the IGMP snooping can work in cooperation with the layer 3 multicast protocols.

21.3.4 IGMP Snooping Troubleshooting

On IGMP Snooping function configuration and usage, IGMP Snooping might not run properly because of physical connection or configuration mistakes. So the users should note that:

- Make sure correct physical connection
- Activate IGMP Snooping on whole configuration mode (use **ip igmp snooping**)
- Configure IGMP Snooping at VLAN on whole configuration mode (use **ip igmp snooping vlan <vlan-id>**)
- Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter
- Use **show ip igmp snooping vlan <vid>** command check IGMP Snooping information

Chapter 22 IPv6 Multicast Protocol

22.1 MLD Snooping

22.1.1 Introduction to MLD Snooping

MLD, the Multicast Listener Discovery Protocol, is used to realize multicasting in the IPv6. MLD is used by the network equipments such as routers which supports multicast for multicast listener discovery, also used by listeners looking forward to join certain multicast group informing the router to receive data packets from certain multicast address, all of which are done through MLD message exchange. First the router send an MLD Multicast listener Query message through a multicast address which can address all the listeners (namely ff02::1). Once there is a listener who wishes to join the multicast address, it will send a MLD Multicast listener Report back through the multicast address.

MLD Snooping is namely the MLD listening. The switch restricts the multicast traffic from flooding through MLD Snooping, and forward the multicast traffic to ports associated to multicast devices only. The switch listens to the MLD messages between multicast routers and listeners, and maintains the multicast group forwarding list based on the listening result. The switches forwards multicast packets according to the multicast forwarding list

The switch realizes the MLD Snooping function while supporting MLD v2. This way, the user can acquire IPv6 multicast with the switch.

22.1.2 MLD Snooping Configuration Task

1. Enable the MLD Snooping function
2. Configure the MLD Snooping

1. Enable the MLD Snooping function

Command	Explanation
Global Mode	
ipv6 mld snooping **no ipv6 mld snooping**	Enable global MLD Snooping, the "**no ipv6 mld snooping**" command disables the global MLD snooping.

2. Configure MLD Snooping

Command	Explanation
Global Mode	

ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable MLD Snooping on specific VLAN. The “no” form of this command disables MLD Snooping on specific VLAN.
ipv6 mld snooping vlan <*vlan-id*> limit {group <*g_limit*> | source <*s_limit*>} **no ipv6 mld snooping vlan <*vlan-id*> limit**	Configure the number of the groups in which the MLD Snooping can join, and the maximum number of sources in each group. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> l2-general-querier **no ipv6 mld snooping vlan <*vlan-id*> l2-general-querier**	Set the VLAN level 2 general querier, which is recommended on each segment. The “no” form of this command cancels the level 2 general querier configuration.
ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Configure the static mrouter port in specific vlan. The “no” form of this command cancels the mrouter port configuration.
ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*> **no ipv6 mld snooping vlan <*vlan-id*> mrpt**	Configure the keep-alive time of the mrouter port. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-interval**	Configure the query interval. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> immediate-leave **no ipv6 mld snooping vlan <*vlan-id*> immediate-leave**	Configure immediate leave multicast group function for the MLD Snooping of specific VLAN. The “no” form of this command cancels the immediate leave configuration.
ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-mrsp**	Configure the query maximum response period. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> query-robustness <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-robustness**	Configure the query robustness, the “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*> **no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time**	Configure the suppression query time. The “no” form of this command restores to the default
Ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source	Configure static-group on specified port of the VLAN. The no form of the command cancels this

<X:X::X:X>] interface [ethernet | port-channel] <IFNAME> **no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>**	configuration.

22.1.3 MLD Snooping Examples

Scenario 1: MLD Snooping Function

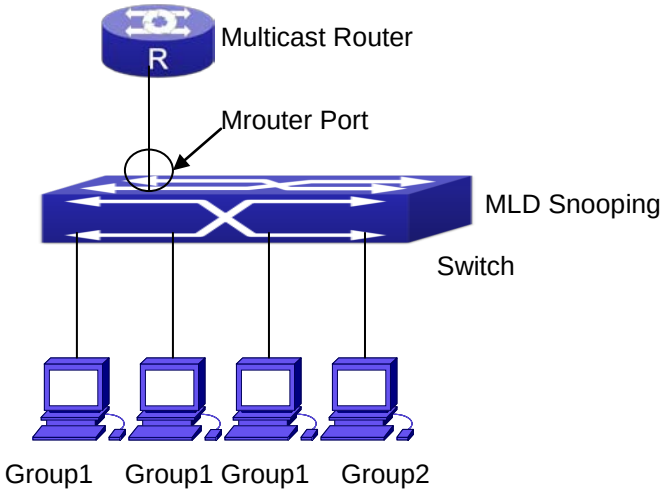


Figure 22-1 Open the switch MLD Snooping Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10, 12. Four hosts are respectively connected to 2, 6, 10, 12 while the multicast router on port 1. Suppose we need MLD Snooping on VLAN 100, however by default, the global MLD Snooping as well as the MLD Snooping on each VLAN are, therefore first we have to enable the global MLD Snooping at the same time enable the MLD Snooping on VLAN 100, furthermore we need to set the port 1 of VLAN 100 as a mrouter port.
Configuration procedure is as follows.

```
Switch#config
Switch(config)#ipv6 mld snooping
Switch(config)#ipv6 mld snooping vlan 100
Switch(config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/1
```

Multicast configuration:
Assume there are two multicast servers: the Multicast Server 1 and the Multicast Server 2, amongst program 1 and 2 are supplied on the Multicast Server 1 while program 3 on the Multicast server 2, using group addresses respectively the Group 1, Group 2 and Group 3. Concurrently multicast application is operating on the four hosts. Two hosts connected to port 2 and 5 are playing program 1 while the host connected to port 10 playing program 2, and the one to port 12 playing program 3.

MLD Snooping interception results:

The multicast table on vlan 100 shows: port1, 2 and 6 are in （Multicasting Server 1, Group1）, port1, 10 are in (Multicasting Server 1,Group2), and port1, 12 are in (Multicasting Server 2, Group3）

All the four hosts successfully receive programs they are interested in. port2, 6 receives no traffic from program2 and 3; port10 receives no traffic from program 1 and 3, and port12 receives no traffic from program1 and 2.

Scenario 2: MLD L2-general-querier

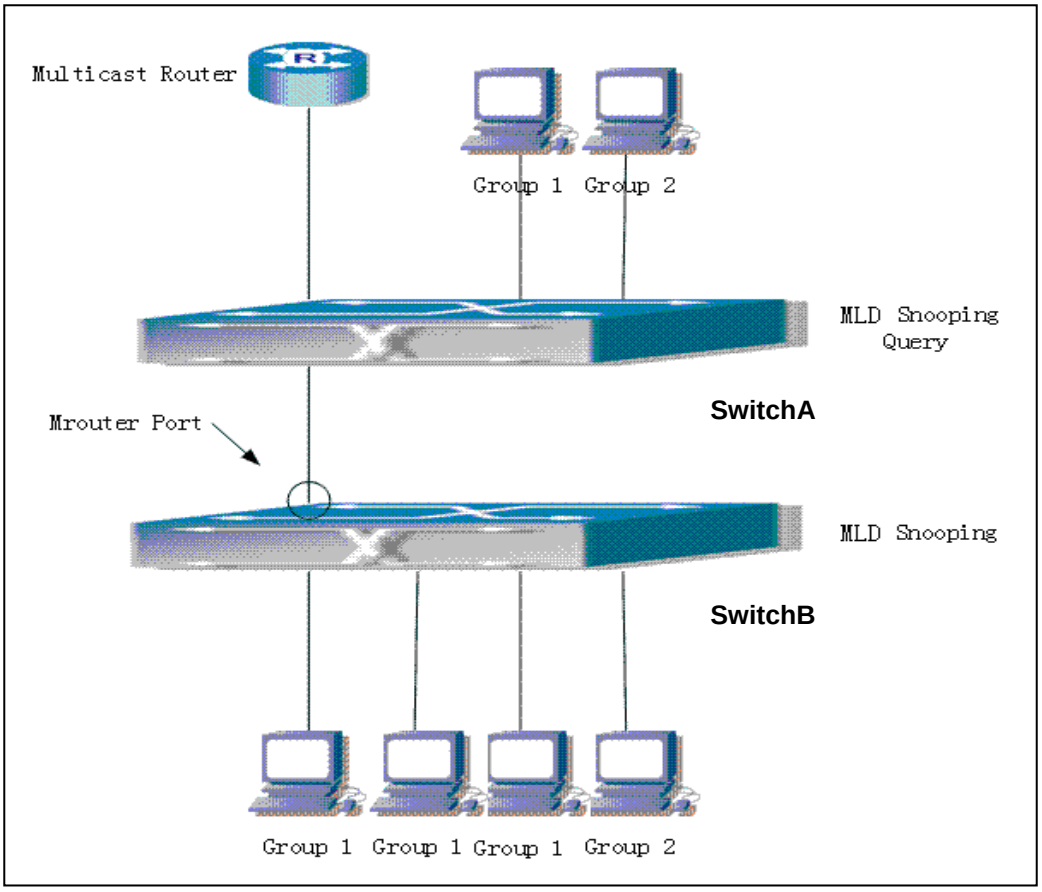


Figure 22-2 Switch as MLD Querier Function figure

Configuration of switch B is the same as the switches in case 1, and here the switch 1 replaces the Multicast Router in case 1. Assume the vlan 60 configured on it contains port 1, 2, 10, 12, amongst port 1 is connected to multicast server, port 2 to switch2. To send Query periodically, global MLD Snooping has to be enabled while executing the mld snooping vlan 60 l2-general-querier, setting the vlan 60 to a Level 2 General Querier. Configuration procedure is as follows:

```
SwitchA#config
SwitchA(config)#ipv6 mld snooping
SwitchA(config)#ipv6 mld snooping vlan 60
SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier
SwitchB#config
SwitchB(config)#ipv6 mld snooping
```

```
SwitchB(config)#ipv6 mld snooping vlan 100
SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/1
```

Multicast configuration:
Same as scenario 1
MLD Snooping interception results:
Same as scenario 1

Scenario 3: To run in cooperation with layer 3 multicast protocols
WITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM6 on ROUTER, and enable PIM-SM6 on vlan 100 (use the same PIM mode with the connected multicast router), the configurations are listed as below:

```
switch#config
switch(config)#ipv6 pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ipv6 pim sparse-mode
```

MLD snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

- To remove the layer 2 multicast entries.
- To provide query functions to the layer 3 with vlan, S, and G as the parameters.
- When layer 3 MLD is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IP6MC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the MLD Snooping can work in cooperation with the layer 3 multicast protocols.

22.1.4 MLD Snooping Troubleshooting

In configuring and using MLD Snooping, the MLD Snooping server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

- Ensure the physical connection is correct
- Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)
- Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>)
- Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,
- Use command to check if the MLD snooping information is correct

Chapter 23 Multicast VLAN

23.1 Introductions to Multicast VLAN

Based on current multicast order method, when orders from users in different VLAN, each VLAN will copy a multicast traffic in this VLAN, which is a great waste of the bandwidth. By configuration of the multicast VLAN, we add the switch port to the multicast VLAN, with the IGMP Snooping/MLD Snooping functions enabled, users from different VLAN will share the same multicast VLAN. The multicast traffic only exists within a multicast VLAN, so the bandwidth is saved. As the multicast VLAN is absolutely separated from the user VLAN, security and bandwidth concerns can be met at the same time, after the multicast VLAN is configured, the multicast traffic will be continuously sent to the users.

23.2 Multicast VLAN Configuration Task List

1 · Enable the multicast VLAN function
2 · Configure the IGMP Snooping
3 · Configure the MLD Snooping

1. Enable the multicast VLAN function

Command	Explanation
VLAN configuration mode	
multicast-vlan **no multicast-vlan**	Configure a VLAN and enable the multicast VLAN on it. The "**no multicast-vlan**" command disables the multicast function on the VLAN.
multicast-vlan association <*vlan-list*> **no multicast-vlan association <*vlan-list*>**	Associate a multicast VLAN with several VLANs. The "no" form of this command deletes the related VLANs associated with the multicast VLAN.

2. Configure the IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enable the IGMP Snooping function on the multicast VLAN. The "no" form of this command disables the IGMP Snooping on the multicast VLAN.
ip igmp snooping **no ip igmp snooping**	Enable the IGMP Snooping function. The "no" form of this command disables the IGMP snooping function.

3. Configure the MLD Snooping

Command	Explanation
Global Mode	
ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable MLD Snooping on multicast VLAN; the “no” form of this command disables MLD Snooping on multicast VLAN.
ipv6 mld snooping **no ipv6 mld snooping**	Enable the MLD Snooping function. The “no” form of this command disables the MLD snooping function.

23.3 Multicast VLAN Examples

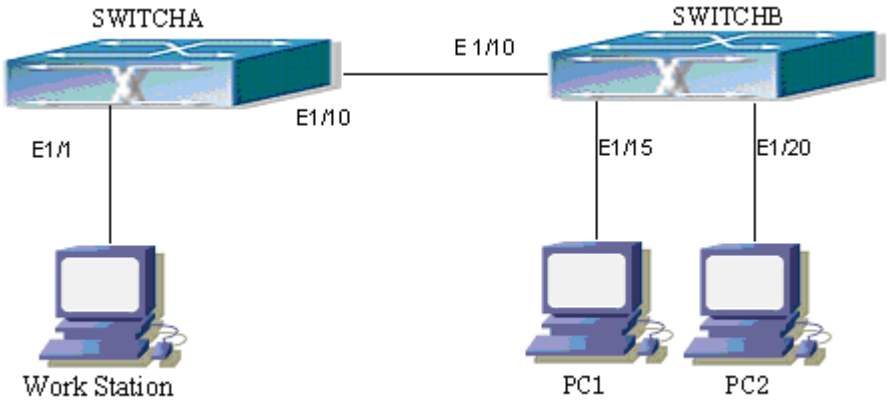


Figure 23-1 Function configuration of the Multicast VLAN

As shown in the figure, the multicast server is connected to the layer 3 switch switchA through port 1/1 which belongs to the VLAN10 of the switch. The layer 3 switch switchA is connected with layer 2 switches through the port1/10, which configured as trunk port. On the switchB the VLAN100 is configured set to contain port1/15, and VLAN101 to contain port1/20. PC1 and PC2 are respectively connected to port 1/15 and1/20. The switchB is connected with the switchA through port1/10, which configured as trunk port. VLAN 20 is a multicast VLAN. By configuring multicast vlan, the PC1 and PC2 will receives the multicast data from the multicast VLAN.

Following configuration is based on the IP address of the switch has been configured and all the equipment are connected correctly.

Configuration procedure

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#switchport access ethernet 1/1
```

```
SwitchA(config-vlan10)exit
SwitchA(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA(config)#ip pim multicast
SwitchA(config)# interface ethernet1/10
SwitchA(Config-If-Ethernet1/10)switchport mode trunk
```

```
SwitchB#config
SwitchB(config)#vlan 100
SwitchB(config-vlan100)#Switchport access ethernet 1/15
SwitchB(config-vlan100)exit
SwitchB(config)#vlan 101
SwitchB(config-vlan101)#Switchport access ethernet 1/20
SwitchB(config-vlan101)exit
SwitchB(config)# interface ethernet 1/10
SwitchB(Config-If-Ethernet1/10)#Switchport mode trunk
SwitchB(Config-If-Ethernet1/10)#exit
SwitchB(config)#vlan 20
SwitchB(config-vlan20)#multicast-vlan
SwitchB(config-vlan20)#multicast-vlan association 100,101
SwitchB(config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

When the multicast VLAN supports the IPv6 multicast, the usage is the same with IPv4, but the difference is using with MLD Snooping, so does not give an example.

Chapter 24 ACL Configuration

24.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming direction of switch ports, so that data streams in the incoming direction of specified ports must comply with the ACL rules assigned.

24.1.1 Access-list

Access-list is a sequential collection of conditions that corresponds to a specific rule. Each rule consist of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port, UDP port. Access-lists can be categorized by the following criteria:

- Filter information based criterion: IP access-list (layer 3 or higher information), MAC access-list (layer 2 information), and MAC-IP access-list (layer 2 or layer 3 or higher).
- Configuration complexity based criterion: standard and extended, the extended mode allows more specific filtering of information.
- Nomenclature based criterion: numbered and named.

Description of an ACL should cover the above three aspects.

24.1.2 Access-group

When a set of access-lists are created, they can be applied to traffic of incoming direction on all ports. Access-group is the description to the binding of an access-list to the incoming direction on a specific port. When an access-group is created, all packets from in the incoming direction through the port will be compared to the access-list rule to decide whether to permit or deny access.
The current firmware only supports ingress ACL configuration.

24.1.3 Access-list Action and Global Default Action

There are two access-list actions and default actions: “permit” or “deny”. The following rules apply:

- An access-list can consist of several rules. Filtering of packets compares packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed.
- Global default action applies only to IP packets in the incoming direction on the ports.
- Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.

24.2 ACL Configuration Task List

ACL Configuration Task Sequence:

1. Configuring access-list
   (1) Configuring a numbered standard IP access-list
   (2) Configuring a numbered extended IP access-list
   (3) Configuring a standard IP access-list based on nomenclature
      a) Create a standard IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   (4) Configuring an extended IP access-list based on nomenclature.
      a) Create an extensive IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries
      c) Exit ACL Configuration Mode
   (5) Configuring a numbered standard MAC access-list
   (6) Configuring a numbered extended MAC access-list
   (7) Configuring a extended MAC access-list based on nomenclature
      a) Create a extensive MAC access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   (8) Configuring a numbered extended MAC-IP access-list
   (9) Configuring a extended MAC-IP access-list based on nomenclature
      a) Create a extensive MAC-IP access-list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit MAC-IP Configuration Mode
   (10) Configuring a numbered standard IPV6 access-list
   (11) Configuring a standard IPV6 access-list based on nomenclature
      a) Create a standard IPV6 access-list based on nomenclature
      b) Specify multiple permit or deny rule entries
      c) Exit ACL Configuration Mode
2. Configuring the packet filtering function
   (2) Enable global packet filtering function
   (3) Configure default action.
3. Configuring time range function
   (4) Create the name of the time range
   (5) Configure periodic time range
   (6) Configure absolute time range
4. Bind access-list to a incoming direction of the specified port
5. Clear the filtering information of the specified port

1. Configuring access-list

(1) Configuring a numbered standard IP access-list

Command	Explanation

Global Mode	
access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} **no access-list <*num*>**	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered standard IP access-list.

(2) Configuring a numbered extensive IP access-list

Command	Explanation
Global Mode	
access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered ICMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
a access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port { <sPort> | range <*sPortMin*> <*sPortMax*> }] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port { <dPort> | range <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered TCP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port { <*sPort*> | range <*sPortMin*> <*sPortMax*> }] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered UDP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <*protocol-num*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the

{{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes a numbered extensive IP access-list.

(3) Configuring a standard IP access-list basing on nomenclature

a. Create a name-based standard IP access-list

Command	Explanation
Global Mode	
ip access-list standard <*name*> **no ip access-list standard <*name*>**	Creates a standard IP access-list based on nomenclature; the "**no ip access-list standard <*name*>**" command deletes the name-based standard IP access-list.

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}	Creates a standard name-based IP access rule; the "**no**" form command deletes the name-based standard IP access rule.

c. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IP ACL Mode	
exit	Exits name-based standard IP ACL configuration mode.

(4) Configuring an name-based extended IP access-list

a. Create an extended IP access-list basing on nomenclature

Command	Explanation
Global Mode	
ip access-list extended <*name*> **no ip access-list extended <*name*>**	Creates an extended IP access-list basing on

	nomenclature; the "**no ip access-list extended <name>** " command deletes the name-based extended IP access-list.

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Extended IP ACL Mode	
[no] {deny | permit} icmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based ICMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule.
[no] {deny | permit} igmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based IGMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule.
[no] {deny | permit} tcp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port { <sPort> | range <*sPortMin*> <*sPortMax*> }] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based TCP IP access rule; the "**no**" form command deletes this name-based extended IP access rule.
[no] {deny | permit} udp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port { <dPort> | range <*dPortMin*> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based UDP IP access rule; the "**no**" form command deletes this name-based extended IP access rule.
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination	Creates an extended name-based IP access rule for other IP protocols; the "**no**" form command deletes this

<*dlpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	name-based extended IP access rule.

c. Exit extended IP ACL configuration mode

Command	Explanation
Extended IP ACL Mode	
exit	Exits extended name-based IP ACL configuration mode.

(5) Configuring a numbered standard MAC access-list

Command	Explanation
Global Mode	
access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} **no access-list <*num*>**	Creates a numbered standard MAC access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered standard MAC access-list.

(6) Creates a numbered MAC extended access-list

Command	Explanation
Global Mode	
access-list<*num*> {deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[{untagged-eth2|tagged-eth2|untagged-802-3|tagged-802-3}] **no access-list <*num*>**	Creates a numbered MAC extended access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered MAC extended access-list.

(7) Configuring a extended MAC access-list based on nomenclature

a. Create a extensive MAC access-list based on nomenclature

Command	Explanation
Global Mode	
mac-access-list extended <*name*>	Creates an extended

no mac-access-list extended <*name*>	name-based MAC access rule for other IP protocols; the "**no**" form command deletes this name-based extended MAC access rule.

b. Specify multiple "permit" or "deny" rule entries

Command	Explanation
Extended name-based MAC access rule Mode	
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>} |{<*dmac*> <*dmac-mask*>}} [cos <*cos-val*> [<*cos-bitmask*>] [vlanId <*vid-value*> [<*vid-mask*>][ethertype<*protocol*>[<*protocol-mask*>]]]] **[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[ethertype<protocol>[<protocol-mask>]]** **[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[vlanId<*vid-value*>[<*vid-mask*>] [ethertype<*protocol*>[<*protocol-mask*>]]]**	Creates an extended name-based MAC access rule matching MAC frame; the "**no**" form command deletes this name-based extended MAC access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]	Creates an extended name-based MAC access rule matching untagged ethernet 2 frame; the "no" form command deletes this name-based extended MAC access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}	Creates an MAC access rule matching 802.3 frame; the "**no**" form command deletes this MAC access rule.

[untagged-802-3]	
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	Creates an MAC access rule matching tagged ethernet 2 frame; the "**no**" form command deletes this MAC access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	Creates an MAC access rule matching tagged 802.3 frame; the "**no**" form command deletes this MAC access rule.

c. Exit ACL Configuration Mode

Command	Explanation
Extended name-based MAC access configure Mode	
exit	Quit the extended name-based MAC access configure mode.

(8) Configuring a numbered extended MAC-IP access-list

Command	Explanation
Global mode	
access-list<*num*>{deny|permit} {any-source-mac| {host-source-mac <*host_smac*>} | {<*smac*> <*smac-mask*>}} {any-destination-mac | {host-destination-mac <*host_dmac*>} | {<*dmac*><*dmac-mask*>}} icmp {{<*source*> <*source-wildcard*>} |any-source| {host-source <*source-host-ip*>}} {{<*destination*> <*destination-wildcard*>} | any-destination | {host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>] [time-range <*time-range-name*>]	Creates a numbered mac-icmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number. Note: switch implement the simple mode of MAC-IP ACL, configure SrcMac+SrcIP or DstMac+DstIP simple mode only.
**access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-ma*	Creates a numbered mac-igmp extended mac-ip

sk>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port { <port1> | range <sPortMin> <sPortMax> }] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port { <port3> | range <sPortMin> <sPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered mac-ip extended mac-tcp access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port { <port1> | range <sPortMin> <sPortMax> }] {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [d-port { <port3> | range <sPortMin> <sPortMax> }] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered mac-udp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source|	Creates a numbered extended mac-ip access rule for other specific mac-ip protocol or all mac-ip protocols; if the numbered extended access-list of

{host-source<*source-host-ip*>} **{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}** **[precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**	specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes this numbered extended MAC-IP access rule.

(9) Configuring a extended MAC-IP access-list based on nomenclature

a. Create a extensive MAC-IP access-list based on nomenclature

Command	Explanation
Global Mode	
mac-ip-access-list extended <*name*> **no mac-ip-access-list extended <*name*>**	Creates an extended name-based MAC-IP access rule; the "**no**" form command deletes this name-based extended MAC-IP access rule.

b. Specify multiple "permit" or "deny" rule entries

Command	Explanation
Extended name-based MAC-IP access Mode	
[no]{deny|permit} **{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}}** **{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp** **{{<*source*><*source-wildcard*>}|any-source|** **{host-source<*source-host-ip*>}}** **{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}}** **[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>][tos<*tos*>][time-range<*time-range-name*>]**	Creates an extended name-based MAC-ICMP access rule; the "**no**" form command deletes this name-based extended MAC-ICMP access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} **{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp**	Creates an extended name-based MAC-IGMP access rule; the "**no**" form command deletes this

{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	name-based extended MAC-IGMP access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port { <port1> | range <*sPortMin*> <*sPortMax*> }] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port { <port3> | range <*sPortMin*> <*sPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence<precedence>][tos<tos>][time-range<*time-range-name*>]	Creates an extended name-based MAC-TCP access rule; the "**no**" form command deletes this name-based extended MAC-TCP access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} [s-port *{* <port1> | range <*sPortMin*> <*sPortMax*> }] {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [d-port { <port3> | range <*sPortMin*> <*sPortMax*> }] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-UDP access rule; the "**no**" form command deletes this name-based extended MAC-UDP access rule.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destinati	Creates an extended name-based access rule for the other IP protocol; the "**no**" form command deletes this name-based extended access rule.

on| {host-destination<*destination-host-ip*>}} [precedence<*precedence*>][tos<*tos*>][time-range<*time-range-name*>]	

c. Exit MAC-IP Configuration Mode

Command	Explanation
Extended name-based MAC-IP access Mode	
exit	Quit extended name-based MAC-IP access mode.

（10） Configuring a numbered standard IPV6 access-list

Command	Explanation
Global Mode	
ipv6 access-list <*num*> {deny | permit} {{<*sIPv6Addr*> <*sPrefixlen*>} | any-source | {host-source <*sIpv6Addr*>}} **no ipv6 access-list <*num*>**	Creates a numbered standard IPV6 access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered standard IPv6 access-list.

（11）Configuring a standard IPV6 access-list based on nomenclature

a. Create a standard IPV6 access-list based on nomenclature

Command	Explanation
Global Mode	
ipv6 access-list standard <*name*> **no ipv6 access-list standard <*name*>**	Creates a standard IP access-list based on nomenclature; the **no** command delete the name-based standard IPV6 access-list.

b. Specify multiple permit or deny rules

Command	Explanation
Standard IPV6 ACL Mode	

[no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <*sIPv6Addr*> }}	Creates a standard name-based IPV6 access rule; the **no** form command deletes the name-based standard IPV6 access rule.

c. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IPV6 ACL Mode	
exit	Exits name-based standard IPV6 ACL configuration mode.

2. Configuring packet filtering function

(1) Enable global packet filtering function

Command	Explanation
Global Mode	
firewall enable	Enables global packet filtering function.
firewall disable	Disables global packet filtering function.

(2) Configure default action.

Command	Explanation
Global Mode	
firewall default {permit |deny}	Sets default action to firewall.

3. Configuring time range function

（1）Create the name of the time range

Command	Explanation
Global Mode	
time-range <*time_range_name*>	Create a time range named time_range_name.
no time-range <*time_range_name*>	Stop the time range function named time_range_name.

（2）Configure periodic time range

Command	Explanation

Time range Mode	
absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <*start_time*> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <*end_time*>	Configure the time range for the request of the week, and every week will run by the time range.
periodic {{Monday+Tuesday+Wednesday+Thursday+ Friday+Saturday+Sunday} | daily | weekdays | weekend} <*start_time*> to <*end_time*>	
[no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <*start_time*> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <*end_time*>	Stop the function of the time range in the week.
[no] periodic {{Monday+Tuesday+Wednesday+Thursday+ Friday+Saturday+Sunday} | daily | weekdays | weekend} <*start_time*> to <*end_time*>	

（3）Configure absolute time range

Command	Explanation
Global Mode	
absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]	Configure absolute time range.
[no] absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]	Stop the function of the time range.

4. Bind access-list to a specific direction of the specified port.

Command	Explanation
Physical Port Mode, VLAN Port Mode	
{ip|ipv6|mac|mac-ip} access-group <*acl-name*> {in}[traffic-statistic] **no {ip|ipv6|mac|mac-ip} access-group <*acl-name*> {in}**	Physical interface mode: Applies an access-list to the specified direction on the port; the no command deletes the access-list bound to the port. VLAN interface mode: Applies an access-list to the specified direction on the

	port of VLAN; the no command deletes the access-list bound to the port of VLAN.

5. Clear the filtering information of the specified port

Command	Explanation
Admin Mode	
clear access-group statistic interface { <interface-name> | ethernet *<interface-name>* }	Clear the filtering information of the specified port.

24.3 ACL Example

Scenario 1:

The user has the following configuration requirement: port 1/10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.

Configuration description:

1 · Create a proper ACL

2 · Configuring packet filtering function

3 · Bind the ACL to the port

The configuration steps are listed below:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#ip access-group 110 in
Switch(Config-If-Ethernet1/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
Firewall status: enable.
Firewall default rule: permit.
Switch#show access-lists
access-list 110(used 1 time(s))
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/10
interface name:Ethernet1/10
the ingress acl use in firewall is 110, traffic-statistics Disable.
```

Scenario 2:

The configuration requirement is stated as below: The switch should drop all the 802.3 datagram with 00-12-11-23-xx-xx as the source MAC address coming from interface 10.

Configuration description:

1 · Create the corresponding access list.

2 · Configure datagram filtering.

3 · Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac
untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#mac access-group 1100 in
Switch(Config-If-Ethernet1/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
   Firewall Status: Enable.
   Firewall Default Rule: Permit.
Switch #show access-lists
access-list 1100(used 1 time(s))
   access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
   untagged-802-3
      access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/10
interface name:Ethernet1/10
    MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

Scenario 3:

The configuration requirement is stated as below: The MAC address range of the network connected to the interface 10 of the switch is 00-12-11-23-xx-xx, and IP network is 10.0.0.0/24. FTP should be disabled and ping requests from outside network should be disabled.

Configuration description:

1 · Create the corresponding access list.

2 · Configure datagram filtering.

3 · Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#mac-ip access-group 3110 in
Switch(Config-Ethernet1/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
   Firewall Status: Enable.
   Firewall Default Rule: Permit.

Switch#show access-lists
     access-list 3110(used 1 time(s))
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
     any-destination-mac
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
          access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch #show access-group interface ethernet 1/10
interface name:Ethernet1/10
     MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

Scenario 4:

The configuration requirement is stated as below: IPv6 protocol runs on the interface 600 of the switch. And the IPv6 network address is 2003:1:1:1::0/64. Users in the 2003:1:1:1:66::0/80 subnet should be disabled from accessing the outside network.

Configuration description:

1 · Create the corresponding access list.

2 · Configure datagram filting.

3 · Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#ipv6 enable
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination
```

```
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
  Firewall Status: Enable.
  Firewall Default Rule: Permit.

Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
  ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
  ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source

Switch #show access-group interface ethernet 1/10
interface name:Ethernet1/10
  IPv6 Ingress access-list used is 600, traffic-statistics Disable.
```

Scenario 5:

The configuration requirement is stated as below: The interface 1, 2, 5, 7 belongs to vlan100, Hosts with 192.168.0.1 as its IP address should be disabled from accessing the listed interfaces.

Configuration description:

1 · Create the corresponding access list.

2 · Configure datagram filtering.

3 · Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch (config)#firewall enable
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/1;2;5;7
Switch (Config-Vlan100)#exit
Switch (config)#access-list 1 deny host-source 192.168.0.1
Switch (config)#interface vlan 100
Switch (Config-if-Vlan100)#ip access-group 1 in
Switch (Config-if-Vlan100)#exit
```

Configuration result:

```
Switch (config)#show access-group interface vlan 100
Interface VLAN 100:
```

```
Ethernet1/1:    IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/2:    IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/5:    IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/7:    IP Ingress access-list used is 1, traffic-statistics Disable.
```

24.4 ACL Troubleshooting

- Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.
- Default rule will be used only if no ACL is bound to the incoming direction of the port, or no ACL entry is matched.
- Each ingress port can bind one MAC-IP ACL, one IP ACL, one MAC ACL, one IPv6 ACL (via the physical interface mode or Vlan interface mode).
- When binding four ACL and packet matching several ACL at the same time, the priority relations are as follows in a top-down order. If the priority is same, then the priority of configuration at first is higher.
    - Ingress IPv6 ACL
    - Ingress MAC-IP ACL
    - Ingress IP ACL
    - Ingress MAC ACL
- The number of ACLs that can be successfully bound depends on the content of the ACL bound and the hardware resource limit. Users will be prompted if an ACL cannot be bound due to hardware resource limitation.
- If an access-list contains same filtering information but conflicting action rules, binding to the port will fail with an error message. For instance, configuring “permit tcp any any-destination” and “deny tcp any any-destination” at the same time is not permitted.
- Viruses such as “worm.blaster” can be blocked by configuring ACL to block specific ICMP packets or specific TCP or UDP port packet.
- If the physical mode of an interface is TRUNK, ACL can only be configured through physical interface mode.
- ACL configured in the physical mode can only be disabled in the physical mode. Those configured in the VLAN interface configuration mode can only be disabled in the VLAN interface mode.
- When a physical interface is added into or removed from a VLAN (with the trunk interfaces as exceptions), ACL configured in the corresponding VLAN will be bound or unbound respectively. If ACL configured in the target VLAN, which is configured in VLAN interface mode, conflicts with existing ACL configuration on the interface, which is configured in physical interface mode, the configuration will fail to effect.
- When no physical interfaces are configured in the VLAN, the ACL configuration of the VLAN will be removed. And it can not recover if new interfaces are added to the VLAN.
- When the interface mode is changed from access mode to trunk mode, the ACL configured in VLAN interface mode which is bound to physical interface will be removed. And when the interface mode is changed from trunk mode to access mode, ACL configured in VLAN1 interface mode will be bound to the physical interface. If binding fails, the changing will fail either.
- When removing a VLAN configuration, if there are any ACLs bound to the VLAN, the ACL will be

removed from all the physical interfaces belonging to the VLAN, and it will be bound to VLAN 1 ACL(if ACL is configured in VLAN1). If VLAN 1 ACL binding fails, the VLAN removal operation will fail.

Chapter 25 802.1x Configuration

25.1 Introduction to 802.1x

The 802.1x protocol originates from 802.11 protocol, the wireless LAN protocol of IEEE, which is designed to provide a solution to doing authentication when users access a wireless LAN. The LAN defined in IEEE 802 LAN protocol does not provide access authentication, which means as long as the users can access a LAN controlling device (such as a LAN Switch), they will be able to get all the devices or resources in the LAN. There was no looming danger in the environment of LAN in those primary enterprise networks.

However, along with the boom of applications like mobile office and service operating networks, the service providers should control and configure the access from user. The prevailing application of WLAN and LAN access in telecommunication networks, in particular, make it necessary to control ports in order to implement the user-level access control. And as a result, IEEE LAN/WAN committee defined a standard, which is 802.1x, to do Port-Based Network Access Control. This standard has been widely used in wireless LAN and ethernet. "Port-Based Network Access Control" means to authenticate and control the user devices on the level of ports of LAN access devices. Only when the user devices connected to the ports pass the authentication, can they access the resources in the LAN, otherwise, the resources in the LAN won't be available.

25.1.1 The Authentication Structure of 802.1x

The system using 802.1x has a typical Client/Server structure, which contains three entities (as illustrated in the next figure): Supplicant system, Authenticator system, and Authentication server system.

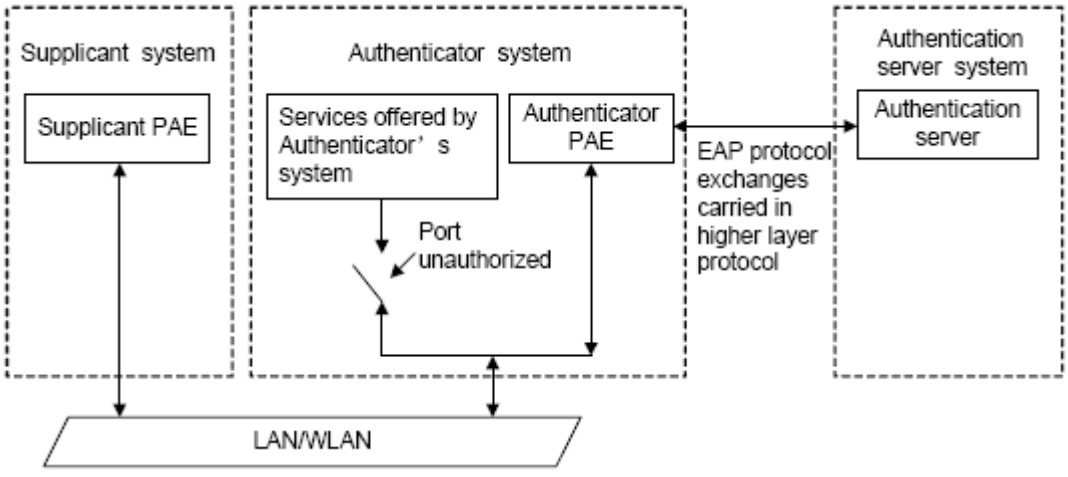


Figure 25-1 The Authentication Structure of 802.1x

- The supplicant system is an entity on one end of the LAN segment, should be authenticated by the access controlling unit on the other end of the link. A Supplicant system usually is a user terminal device. Users start 802.1x authentication by starting supplicant system software. A supplicant system should support EAPOL (Extensible Authentication Protocol over LAN).

- The authenticator system is another entity on one end of the LAN segment to authenticate the supplicant systems connected. An authenticator system usually is a network device supporting 802,1x protocol, providing ports to access the LAN for supplicant systems. The ports provided can either be physical or logical.
- The authentication server system is an entity to provide authentication service for authenticator systems. The authentication server system is used to authenticate and authorize users, as well as does fee-counting, and usually is a RADIUS (Remote Authentication Dial-In User Service) server, which can store the relative user information, including username, password and other parameters such as the VLAN and ports which the user belongs to.

The three entities above concerns the following basic concepts: PAE of the port, the controlled ports and the controlled direction.

1. PAE

PAE (Port Access Entity) is the entity to implement the operation of algorithms and protocols.

- The PAE of the supplicant system is supposed to respond the authentication request from the authenticator systems and submit user's authentication information to the authenticator system. It can also send authentication request and off-line request to authenticator.
- The PAE of the authenticator system authenticates the supplicant systems needing to access the LAN via the authentication server system, and deal with the authenticated/unauthenticated state of the controlled port according to the result of the authentication. The authenticated state means the user is allowed to access the network resources, the unauthenticated state means only the EAPOL messages are allowed to be received and sent while the user is forbidden to access network resources.

2. controlled/uncontrolled ports

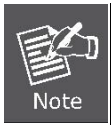
The authenticator system provides ports to access the LAN for the supplicant systems. These ports can be divided into two kinds of logical ports: controlled ports and uncontrolled ports.

- The uncontrolled port is always in bi-directionally connected status, and mainly used to transmit EAPOL protocol frames, to guarantee that the supplicant systems can always send or receive authentication messages.
- The controlled port is in connected status authenticated to transmit service messages. When unauthenticated, no message from supplicant systems is allowed to be received.
- The controlled and uncontrolled ports are two parts of one port, which means each frame reaching this port is visible on both the controlled and uncontrolled ports.

3. Controlled direction

In unauthenticated status, controlled ports can be set as unidirectional controlled or bi-directionally controlled.

- When the port is bi-directionally controlled, the sending and receiving of all frames is forbidden.
- When the port is unidirectional controlled, no frames can be received from the supplicant systems while sending frames to the supplicant systems is allowed.



At present, this kind of switch only supports unidirectional control.

25.1.2 The Work Mechanism of 802.1x

IEEE 802.1x authentication system uses EAP (Extensible Authentication Protocol) to implement exchange of authentication information between the supplicant system, authenticator system and authentication server system.

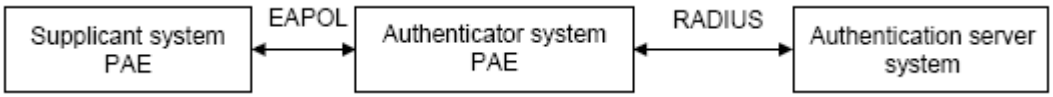


Figure 25-2 the Work Mechanism of 802.1x

- EAP messages adopt EAPOL encapsulation format between the PAE of the supplicant system and the PAE of the authenticator system in the environment of LAN.
- Between the PAE of the authenticator system and the RADIUS server, there are two methods to exchange information: one method is that EAP messages adopt EAPOR (EAP over RADIUS) encapsulation format in RADIUS protocol; the other is that EAP messages terminate with the PAE of the authenticator system, and adopt the messages containing RAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attributes to do the authentication interaction with the RADIUS server.
- When the user pass the authentication, the authentication server system will send the relative information of the user to authenticator system, the PAE of the authenticator system will decide the authenticated/unauthenticated status of the controlled port according to the authentication result of the RADIUS server.

25.1.3 The Encapsulation of EAPOL Messages

1. The Format of EAPOL Data Packets

EAPOL is a kind of message encapsulation format defined in 802.1x protocol, and is mainly used to transmit EAP messages between the supplicant system and the authenticator system in order to allow the transmission of EAP messages through the LAN. In IEEE 802/Ethernet LAN environment, the format of EAPOL packet is illustrated in the next figure. The beginning of the EAPOL packet is the Type/Length domain in MAC frames.

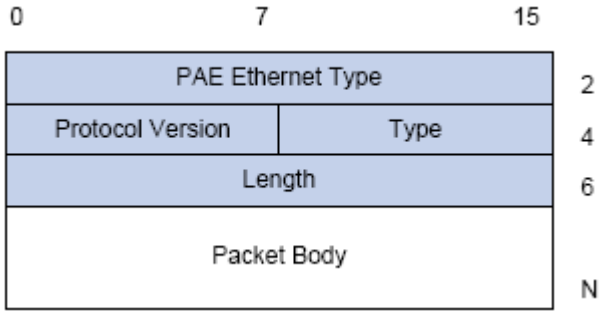


Figure 25-3 the Format of EAPOL Data Packet

PAE Ethernet Type: Represents the type of the protocol whose value is 0x888E.
Protocol Version: Represents the version of the protocol supported by the sender of EAPOL data packets.
Type: represents the type of the EAPOL data packets, including:

- EAP-Packet (whose value is 0x00): the authentication information frame, used to carry EAP messages. This kind of frame can pass through the authenticator system to transmit EAP messages between the supplicant system and the authentication server system.
- EAPOL-Start (whose value is 0x01): the frame to start authentication.
- EAPOL-Logoff (whose value is 0x02): the frame requesting to quit.
- EAPOL-Key (whose value is 0x03): the key information frame.
- EAPOL-Encapsulated-ASF-Alert (whose value is 0x04): used to support the Alerting messages of ASF (Alert Standard Forum). This kind of frame is used to encapsulate the relative information of network management such as all kinds of alerting information, terminated by terminal devices.

Length: represents the length of the data, that is, the length of the “Packet Body”, in byte. There will be no following data domain when its value is 0.
Packet Body: represents the content of the data, which will be in different formats according to different types.

2. The Format of EAP Data Packets

When the value of Type domain in EAPOL packet is EAP-Packet, the Packet Body is in EAP format (illustrated in the next figure).

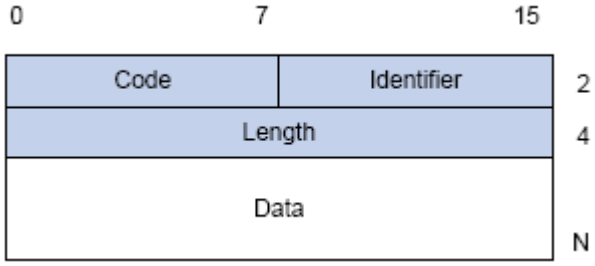


Figure 25-4 the Format of EAP Data Packets

Code: specifies the type of the EAP packet. There are four of them in total: Request（1）,Response（2）,Success（3）,Failure（4）.

- There is no Data domain in the packets of which the type is Success or Failure, and the value of the Length domains in such packets is 4.
- The format of Data domains in the packets of which the type is Request and Response is illustrated in the next figure. Type is the authentication type of EAP, the content of Type data depends on the type. For example, when the value of the type is 1, it means Identity, and is used to query the identity of the other side. When the type is 4, it means MD5-Challenge, like PPP CHAP protocol, contains query messages.

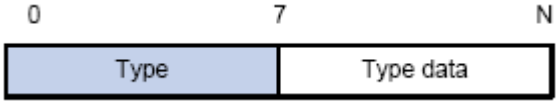


Figure 25-5 the Format of Data Domain in Request and Response Packets

Identifier: to assist matching the Request and Response messages.

Length: the length of the EAP packet, covering the domains of Code, Identifier, Length and Data, in byte.

Data: the content of the EAP packet, depending on the Code type.

25.1.4 The Encapsulation of EAP Attributes

RADIUS adds two attribute to support EAP authentication: EAP-Message and Message-Authenticator. Please refer to the Introduction of RADIUS protocol in “AAA-RADIUS-HWTACACS operation” to check the format of RADIUS messages.

1. EAP-Message

As illustrated in the next figure, this attribute is used to encapsulate EAP packet, the type code is 79, String domain should be no longer than 253 bytes. If the data length in an EAP packet is larger than 253 bytes, the packet can be divided into fragments, which then will be encapsulated in several EAP-Messages attributes in their original order.

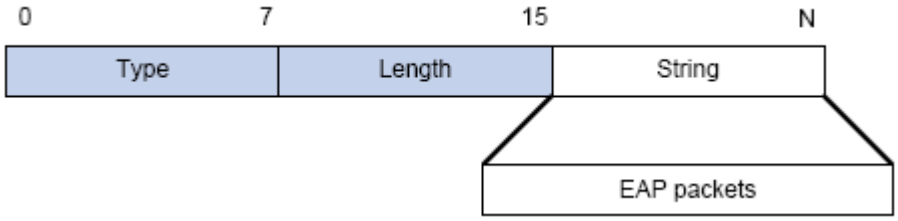


Figure 25-6 the Encapsulation of EAP-Message Attribute

2. Message-Authenticator

As illustrated in the next figure, this attribute is used in the process of using authentication methods like EAP and CHAP to prevent the access request packets from being eavesdropped. Message-Authenticator should be included in the packets containing the EAP-Message attribute, or the packet will be dropped as an invalid one.

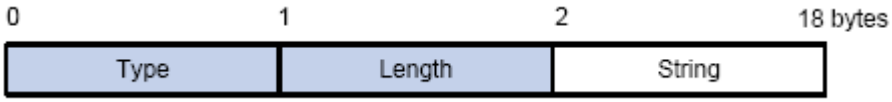


Figure 25-7 Message-Authenticator Attribute

25.1.5 Web Authentication Proxy based on 802.1x

The perspective of prior 802.1x authentication system abided by IEEE 802.1 x authentication systems on architecture, working mechanism, business processes. The client authentication pattern of prior authentication system privately. The devices are layer 2 switch and the authentication server is RADIUS server. EAP protocol is used for the authentication message pattern. EAPOL encapsulation is used between

client and the authentication proxy switch, that is to say, EAP message is encapsulated in the Ethernet frame to authenticate and communicate, however, EAPOR encapsulation is used between authentication proxy switch and authentication server, that is to say, EAP message is loaded on the Radius protocol to authenticate and communicate. it can be also forward by the device, transmit the PAP protocol message or CHAP protocol message based on the RADIUS protocol between the device and the RADIUS sever.

In 802.1x authentication system, in order to implement the identity authentication and the network permission, user should install the authentication client software, pass client login authentication progress and then achieve authenticated communication with DCBI server. But some customers do not want to install client software, and they hope to authenticate by the internet explorer simplified. So in order to satisfy the new demand from the user and realize the platforms irrelevance of the authentication client, the Web authentication function based on 802.1x is designed for authentication.

The Web authentication is still based on IEEE 802.1x authentication system, the Java Applet in internet explorer is instead of the prior client software, the devises is layer 3 switch, authentication server is the standardized RADIUS server, and the authentication message is loaded in the EAP message to communicate. The Ethernet frame can't be send because of the Java Applet used in client, so EAP message can't be encapsulated in the Ethernet frame to send, EAP message should be loaded on the UDP protocol instead of EAPOU, in order to achieve the authentication and communication between web client and web authentication proxy switch. The standardized EAPOR protocol is still used between the authentication proxy switch and authentication server.

25.1.6 The Authentication Methods of 802.1x

The authentication can either be started by supplicant system initiatively or by devices. When the device detects unauthenticated users to access the network, it will send supplicant system EAP-Request/Identity messages to start authentication. On the other hand, the supplicant system can send EAPOL-Start message to the device via supplicant software.

802.1 x systems supports EAP relay method and EAP termination method to implement authentication with the remote RADIUS server. The following is the description of the process of these two authentication methods, both started by the supplicant system.

25.1.6.1 EAP Relay Mode

EAP relay is specified in IEEE 802.1x standard to carry EAP in other high-level protocols, such as EAP over RADIUS, making sure that extended authentication protocol messages can reach the authentication server through complicated networks. In general, EAP relay requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator.

EAP is a widely-used authentication frame to transmit the actual authentication protocol rather than a special authentication mechanism. EAP provides some common function and allows the authentication mechanisms expected in the negotiation, which are called EAP Method. The advantage of EAP lies in that EAP mechanism working as a base needs no adjustment when a new authentication protocol appears. The following figure

illustrates the protocol stack of EAP authentication method.

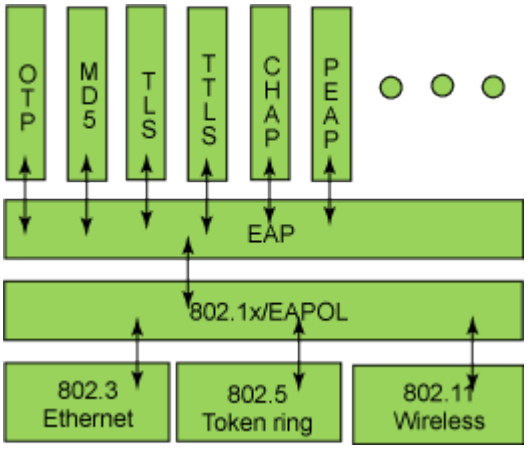


Figure 25-8 the Protocol Stack of EAP Authentication Method

By now, there are more than 50 EAP authentication methods has been developed, the differences among which are those in the authentication mechanism and the management of keys. The 4 most common EAP authentication methods are listed as follows:

- **EAP-MD5**
- **EAP-TLS**（Transport Layer Security）
- **EAP-TTLS**（Tunneled Transport Layer Security）
- **PEAP**（Protected Extensible Authentication Protocol）

They will be described in detail in the following part.

Attention:

- The switch, as the access controlling unit of Pass-through, will not check the content of a particular EAP method, so can support all the EAP methods above and all the EAP authentication methods that may be extended in the future.
- In EAP relay, if any authentication method in EAP-MD5, EAP-TLS, EAP-TTLS and PEAP is adopted, the authentication methods of the supplicant system and the RADIUS server should be the same.

1. EAP-MD5 Authentication Method

EAP-MD5 is an IETF open standard which providing the least security, since MD5 Hash function is vulnerable to dictionary attacks.

The following figure illustrated the basic operation flow of the EAP-MD5 authentication method.

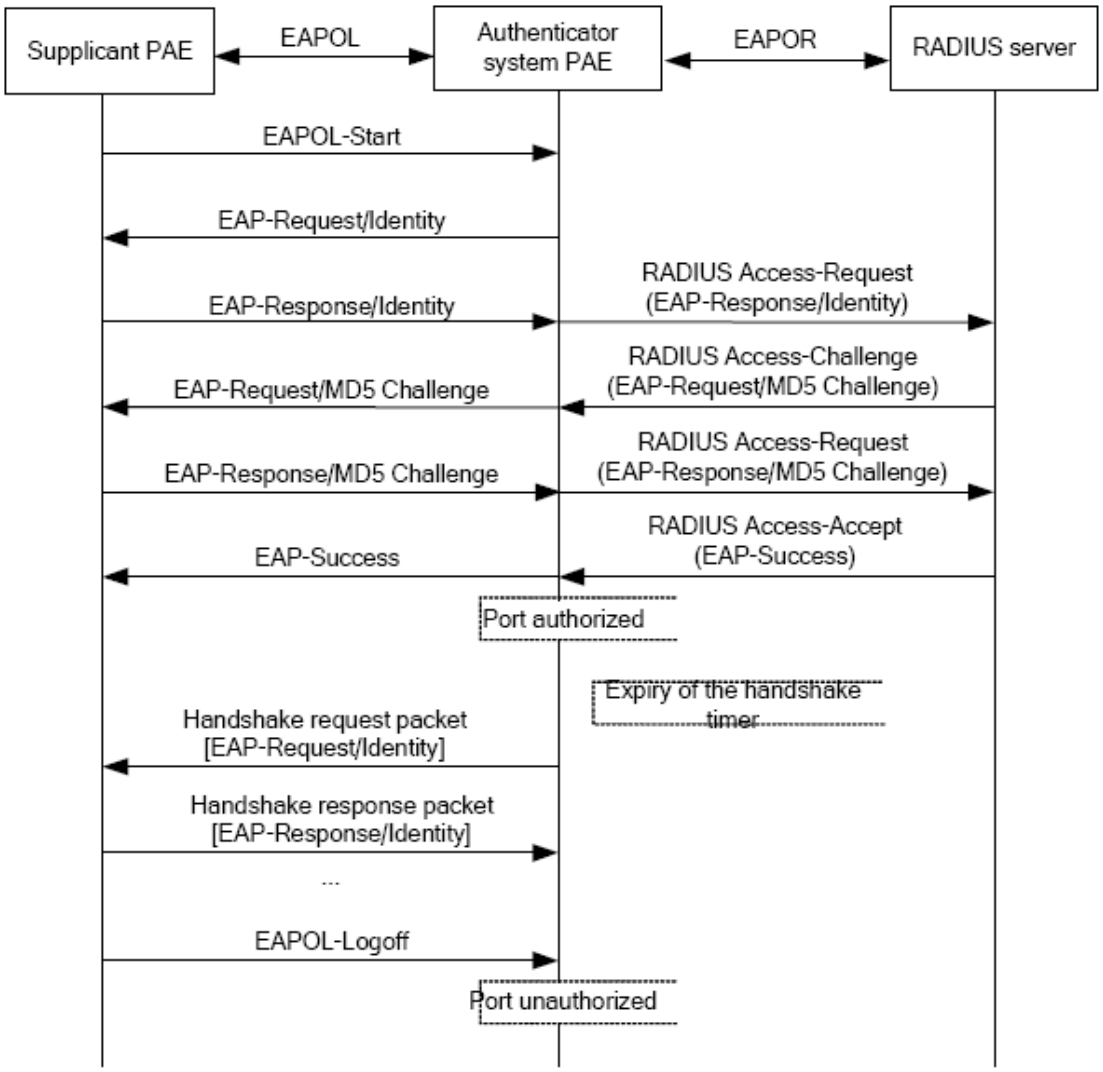


Figure 25-9 the Authentication Flow of 802.1x EAP-MD5

2. EAP-TLS Authentication Method

EAP-TLS is brought up by Microsoft based on EAP and TLS protocols. It uses PKI to protect the id authentication between the supplicant system and the RADIUS server and the dynamically generated session keys, requiring both the supplicant system and the Radius authentication server to possess digital certificate to implement bidirectional authentication. It is the earliest EAP authentication method used in wireless LAN. Since every user should have a digital certificate, this method is rarely used practically considering the difficult maintenance. However it is still one of the safest EAP standards, and enjoys prevailing supports from the vendors of wireless LAN hardware and software.

The following figure illustrates the basic operation flow of the EAP-TLS authentication method.

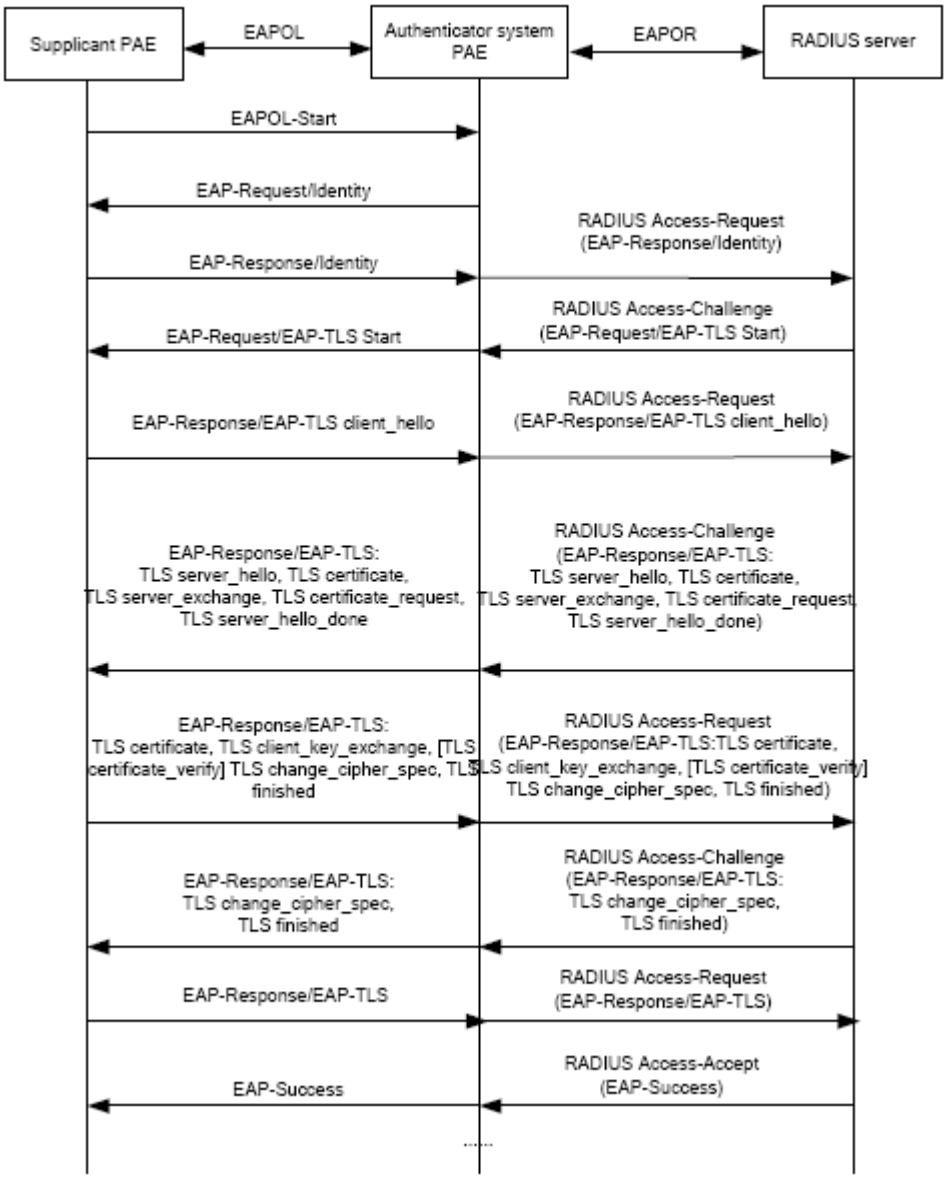


Figure 25-10 the Authentication Flow of 802.1x EAP-TLS

3. EAP-TTLS Authentication Method

EAP-TTLS is a product of the cooperation of Funk Software and Certicom. It can provide an authentication as strong as that provided by EAP-TLS, but without requiring users to have their own digital certificate. The only request is that the Radius server should have a digital certificate. The authentication of users' identity is implemented with passwords transmitted in a safely encrypted tunnel established via the certificate of the authentication server. Any kind of authentication request including EAP, PAP and MS-CHAPV2 can be transmitted within TTLS tunnels.

4. PEAP Authentication Method

EAP-PEAP is brought up by Cisco, Microsoft and RAS Security as a recommended open standard. It has long been utilized in products and provides very good security. Its design of protocol and security is similar to that of EAP-TTLS, using a server's PKI certificate to establish a safe TLS tunnel in order to protect user authentication.

The following figure illustrates the basic operation flow of PEAP authentication method.

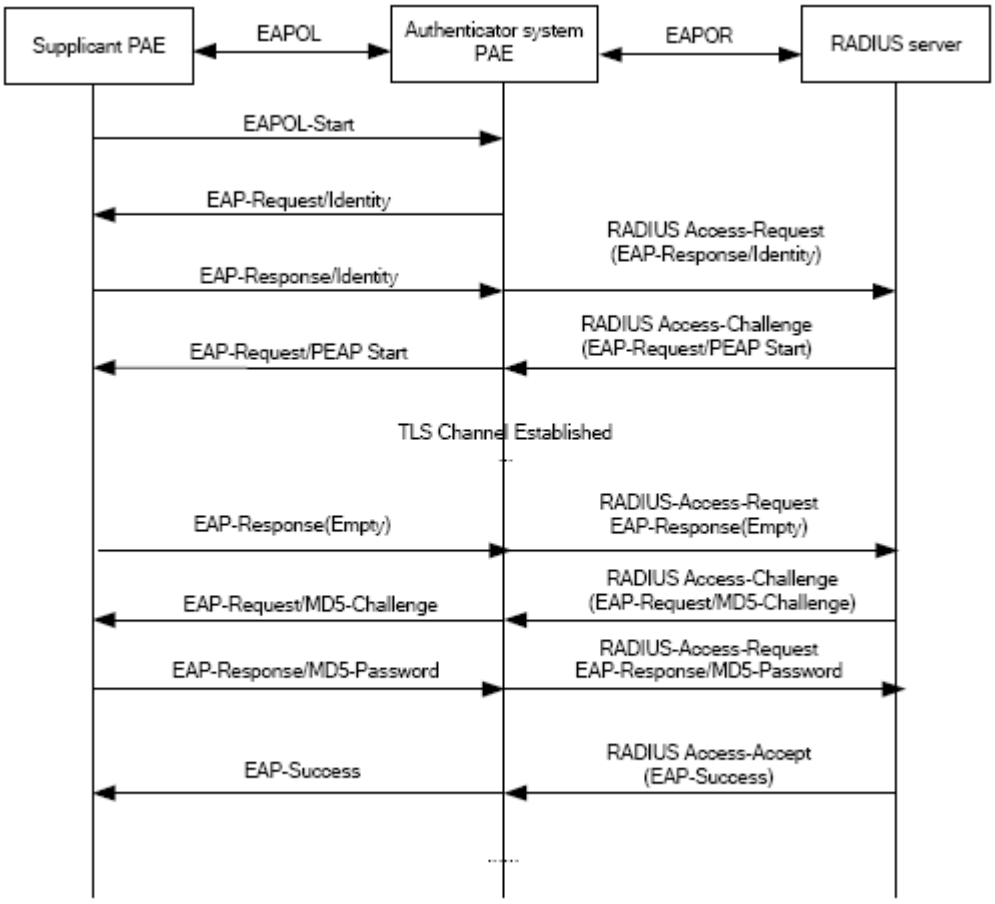


Figure 25-11 the Authentication Flow of 802.1x PEAP

25.1.6.2 EAP Termination Mode

In this mode, EAP messages will be terminated in the access control unit and mapped into RADIUS messages, which is used to implement the authentication, authorization and fee-counting. The basic operation flow is illustrated in the next figure.

In EAP termination mode, the access control unit and the RADIUS server can use PAP or CHAP authentication method. The following figure will demonstrate the basic operation flow using CHAP authentication method.

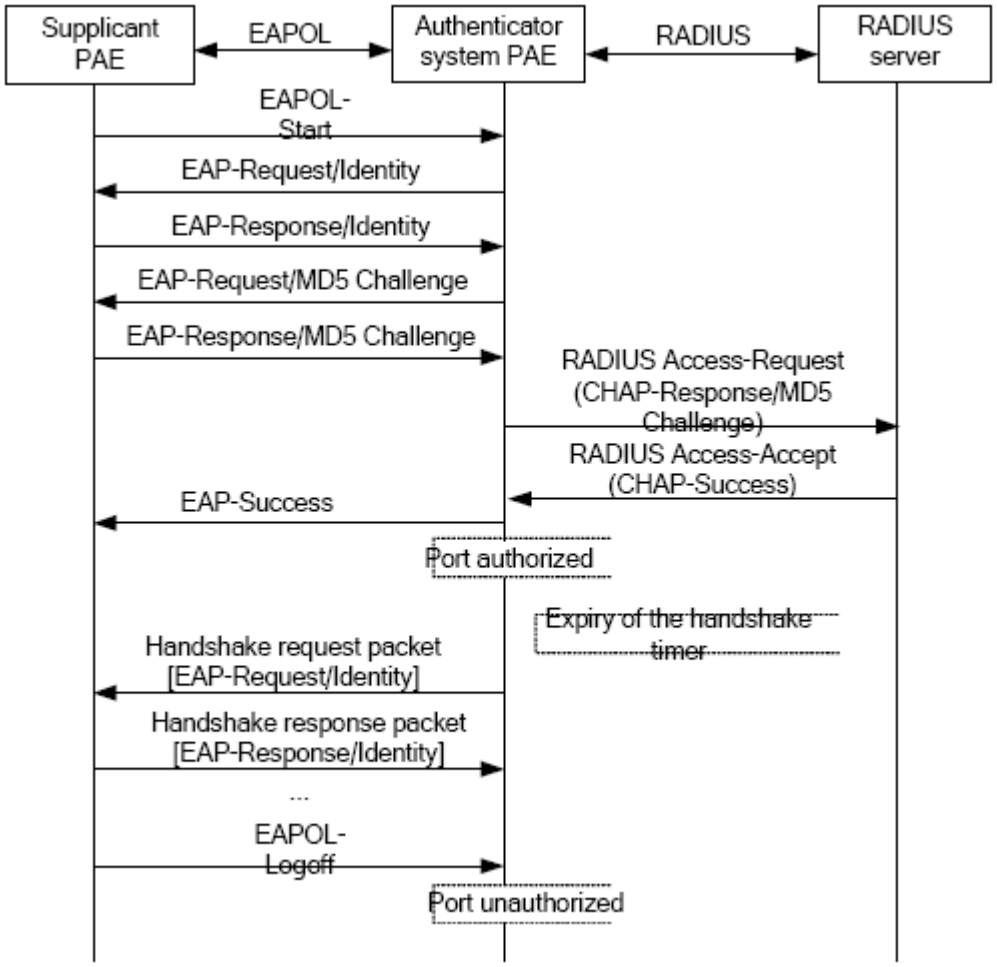


Figure 25-12 the Authentication Flow of 802.1x EAP Termination Mode

25.1.7 The Extension and Optimization of 802.1x

Besides supporting the port- based access authentication method specified by the protocol, devices also extend and optimize it when implementing the EAP relay mode and EAP termination mode of 802.1x.

- Supports some applications in the case of which one physical port can have more than one users
- There are three access control methods (the methods to authenticate users): port-based, MAC-based and user-based (IP address+ MAC address+ port).
  - When the port-based method is used, as long as the first user of this port passes the authentication, all the other users can access the network resources without being authenticated. However, once the first user is offline, the network won't be available to all the other users.
  - When the MAC-based method is used, all the users accessing a port should be authenticated separately, only those pass the authentication can access the network, while the others can not. When one user becomes offline, the other users will not be affected.
  - When the user-based (IP address+ MAC address+ port) method is used, all users can access limited resources before being authenticated. There are two kinds of control in this method: standard control and advanced control. The user-based standard control will not restrict the access to limited resources, which means all users of this port can access limited resources before being

authenticated. The user-based advanced control will restrict the access to limited resources, only some particular users of the port can access limited resources before being authenticated. Once those users pass the authentication, they can access all resources.

Attention: when using private supplicant systems, user-based advanced control is recommended to effectively prevent ARP cheat.

The maximum number of the authenticated users can be 4000, but less than 2000 will be preferred.

25.1.8 The Features of VLAN Allocation

1. Auto VLAN

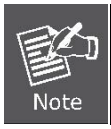
Auto VLAN feature enables RADIUS server to change the VLAN to which the access port belongs, based on the user information and the user access device information. When an 802.1x user passes authentication on the server, the RADIUS server will send the authorization information to the device, if the RADIUS server has enabled the VLAN-assigning function, then the following attributes should be included in the Access-Accept messages:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802 (6)
- Tunnel-Private-Group-ID = VLANID

The VLANID here means the VID of VLAN, ranging from 1 to 4094. For example, Tunnel-Private-Group-ID = 30 means VLAN 30.

When the switch receives the assigned Auto VLAN information, the current Access port will leave the VLAN set by the user and join Auto VLAN.

Auto VLAN won't change or affect the port's configuration. But the priority of Auto VLAN is higher than that of the user-set VLAN, that is Auto VLAN is the one takes effect when the authentication is finished, while the user-set VLAN do not work until the user become offline.



At present, Auto VLAN can only be used in the port-based access control mode, and on the ports whose link type is Access.

2. Guest VLAN

Guest VLAN feature is used to allow the unauthenticated user to access some specified resources.

The user authentication port belongs to a default VLAN (Guest VLAN) before passing the 802.1x authentication, with the right to access the resources within this VLAN without authentication. But the resources in other networks are beyond reach. Once authenticated, the port will leave Guest VLAN, and the user can access the resources of other networks.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being

too low.

Once the 802.1x feature is enabled and the Guest VLAN is configured properly, a port will be added into Guest VLAN, just like Auto VLAN, if there is no response message from the supplicant system after the device sends more authentication-triggering messages than the upper limit (EAP-Request/Identity) from the port.

- The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the assigned Auto VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.
- The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

25.2 802.1x Configuration Task List

802.1x Configuration Task List:

1. Enable IEEE 802.1x function
2. Configure web authentication agent function
   3. Access management unit property configuration
   1) Configure port authentication status
   2) Configure access management method for the port: MAC-based or port-based.
   3) Configure expanded 802.1x function
   4) Configure IPv6 passthrough function of the port
4. User access devices related property configuration (optional)

1. Enable 802.1x function

Command	Explanation
Global Mode	
dot1x enable **no dot1x enable**	Enables the 802.1x function in the switch and ports; the no command disables the 802.1x function.
dot1x privateclient enable **no dot1x privateclient enable**	Enables the switch force client software using private 802.1x authentication packet format. The no command will disable this function.
dot1x user free-resource ***<prefix> <mask>*** **no dot1x user free-resource**	Sets free access network resource for unauthorized dot1x user. The no command close the resource.

2. Configure Web authentication agent function

Command	Explanation
Global Mode	

dot1x web authentication enable ***no* dot1x web authentication enable**	Enable Web authentication agent, the no command disable Web authentication agent.
dot1x web redirect <*URL*> **no dot1x web redirect**	Set the HTTP server address for Web redirection, the no command clears the address.

3. Access management unit property configuration

1) Configure port authentication status

Command	Explanation
Port Mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Sets the 802.1x authentication mode; the no command restores the default setting.

2) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method {macbased | portbased |webbased|userbased advanced} **no dot1x port-method**	Sets the port access management method; the no command restores MAC-based access management.
dot1x max-user macbased <*number*> **no dot1x max-user macbased**	Sets the maximum number of access users for the specified port; the no command restores the default setting of allowing 1 user.
dot1x max-user userbased <number> **no dot1x max-user userbased**	Set the upper limit of the number of users allowed accessing the specified port, only used when the access control mode of the port is userbased; the no command is used to reset the limit to 10 by default.
dot1x guest-vlan <vlanID> **no dot1x guest-vlan**	Set the guest vlan of the specified port; the no command is used to delete the guest vlan.

3) Configure expanded 802.1x function

Command	Explanation
Global Mode	
dot1x macfilter enable **no dot1x macfilter enable**	Enables the 802.1x address filter function in the switch; the no command disables the 802.1x address filter function.

dot1x accept-mac <mac-address> [interface <interface-name>] **no dot1x accept-mac <mac-address> [interface <interface-name>]**	Adds 802.1x address filter table entry, the no command deletes 802.1x filter address table entries.
dot1x eapor enable **no dot1x eapor enable**	Enables the EAP relay authentication function in the switch; the no command sets EAP local end authentication.

4) Configure IPv6 passthrough function of the port

Command	Explanation
Global Mode	
dot1x ipv6 passthrough **no dot1x *ipv6* passthrough**	Enables IPv6 passthrough function of global mode on a switch, only applicable when access control mode is userbased; the no operation of this command will disable the function.
dot1x web authentication ipv6 passthrough **no dot1x web authentication ipv6 passthrough**	Enable IPv6 passthrough function on a switch port, only applicable when access control mode is webbased; the no operation of this command will disable the function.

4. Supplicant related property configuration

Command	Explanation
Global Mode	
dot1x max-req <count> **no dot1x max-req**	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the no command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the no command disables this function.
dot1x timeout quiet-period <seconds> **no dot1x timeout quiet-period**	Sets time to keep silent on port authentication failure; the no command restores the default value.
dot1x timeout re-authperiod <seconds> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the no command restores the default setting.
dot1x timeout tx-period <seconds> **no dot1x timeout tx-period**	Sets the interval for the supplicant to re-transmit EAP request/identity frame; the no command restores the default setting.

dot1x re-authenticate [interface <interface-name>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

25.3 802.1x Application Example

25.3.1 Examples of Guest Vlan Applications

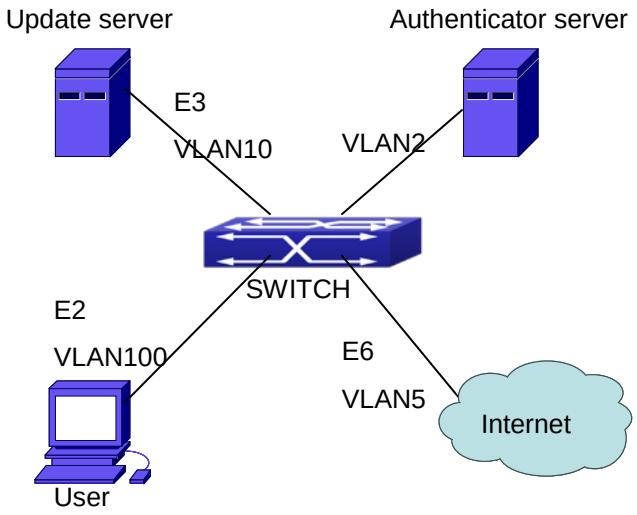


Figure 25-13 The Network Topology of Guest VLAN

Note	in the figures in this session, E2 means Ethernet 1/2, E3 means Ethernet 1/3 and E6 means Ethernet 1/6.

As showed in the next figure, a switch accesses the network using 802.1x authentication, with a RADIUS server as its authentication server. Ethernet1/2, the port through which the user accesses the switch belongs to VLAN100; the authentication server is in VLAN2; Update Server, being in VLAN10, is for the user to download and update supplicant system software; Ethernet1/6, the port used by the switch to access the Internet is in VLAN5.

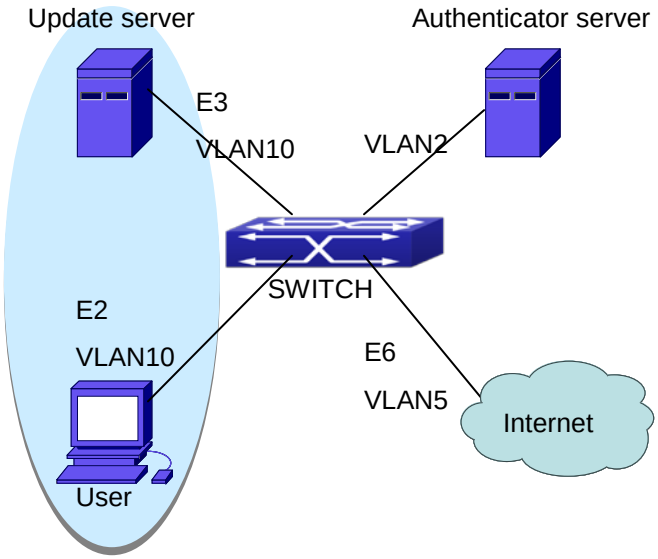


Figure 25-14 User Joining Guest VLAN

As illustrated in the up figure, on the switch port Ethernet1/2, the 802.1x feature is enabled, and the VLAN10 is set as the port's Guest VLAN. Before the user gets authenticated or when the user fails to do so, port Ethernet1/2 is added into VLAN10, allowing the user to access the Update Server.

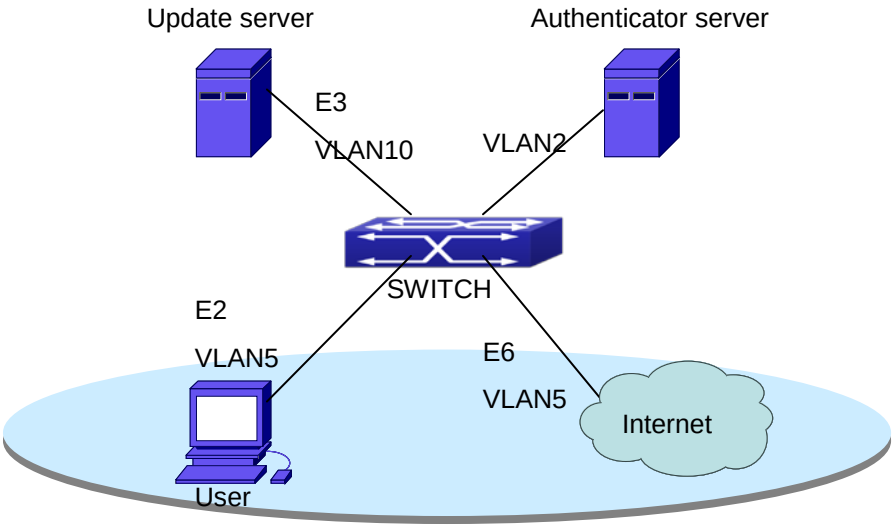


Figure 25-15 User Being Online, VLAN Being Offline

As illustrated in the up figure, when the users become online after a successful authentication, the authentication server will assign VLAN5, which makes the user and Ethernet1/6 both in VLAN5, allowing the user to access the Internet.

The following are configuration steps:

```
# Configure RADIUS server.
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

# Create VLAN100.
Switch(config)#vlan 100

# Enable the global 802.1x function
Switch(config)#dot1x enable

# Enable the 802.1x function on port Ethernet1/2
Switch(config)#interface ethernet1/2
Switch(Config-If-Ethernet1/2)#dot1x enable

# Set the link type of the port as access mode.
Switch(Config-If-Ethernet1/2)#switch-port mode access

# Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/2)#dot1x port-method portbased

# Set the access control mode on the port as auto.
Switch(Config-If-Ethernet1/2)#dot1x port-control auto

# Set the port's Guest VLAN as 100.
Switch(Config-If-Ethernet1/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/2)#exit
```

Using the command of **show running-config** or **show interface ethernet 1/2**, users can check the configuration of Guest VLAN. When there is no online user, no failed user authentication or no user gets offline successfully, and more authentication-triggering messages (EAP-Request/Identity) are sent than the upper limit defined, users can check whether the Guest VLAN configured on the port takes effect with the command **show vlan id 100**.

25.3.2 Examples of IPv4 Radius Applications

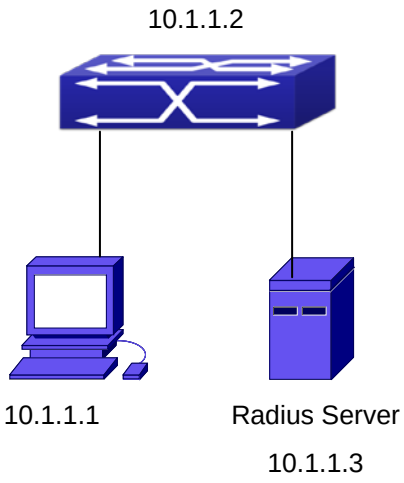


Figure 25-16 IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/2 of the switch; IEEE 802.1x authentication is enabled on port1/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/2 is used to connect to RADIUS authentication server, which has an IP address of 10.1.1.3, and use the default port 1812 for authentication and port 1813 for accounting. IEEE 802.1x authentication client software is installed on the PC and is used in IEEE 802.1x authentication.
The configuration procedures are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#dot1x enable
Switch(Config-If-Ethernet1/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/2)#exit
```

25.3.3 Examples of IPv6 Radius Application

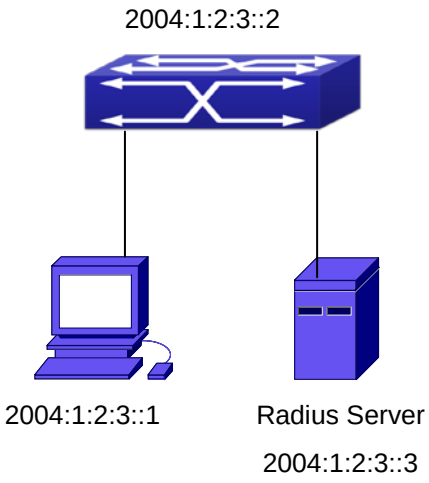


Figure 25-17 IPv6 Radius

Connect the computer to the interface 1/2 of the switch, and enable IEEE802.1x on interface1/2. Use MAC based authentication. Configure the IP address of the switch as 2004:1:2:3::2, and connect the switch with any interface except interface 1/2 to the RADIUS authentication server. Configure the IP address of the RADIUS server to be 2004:1:2:3::3. Use the default ports 1812 and 1813 for authentication and accounting respectively. Install the IEEE802.1x authentication client software on the computer, and use the client for IEEE802.1x authentication.

The detailed configurations are listed as below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#dot1x enable
Switch(Config-If-Ethernet1/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/2)#exit
```

25.3.4 802.1x Web Proxy Authentication Sample Application

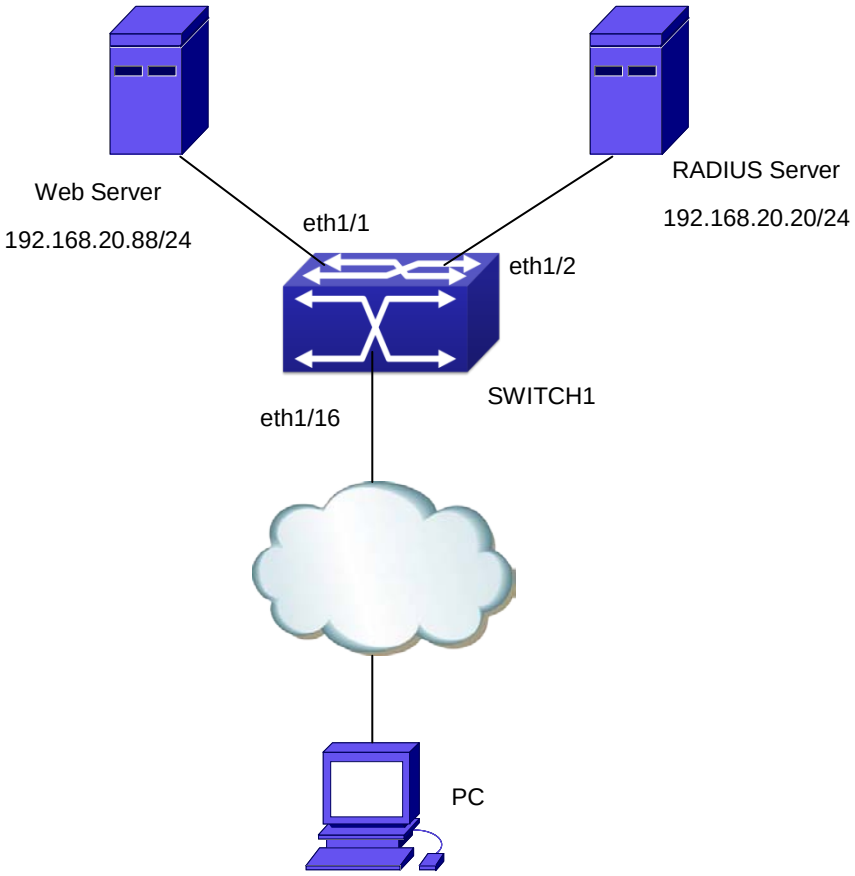


Figure 25-18 802.1x Web Proxy Authentication

In the network topology shown as above, Ethernet 1/1 on SWITCH1 is connected to the Web server whose IP address is 192.168.20.20/24, Ethernet 1/2 on SWITCH1 is connected to the RADIUS server whose IP address is 192.168.20.88/24 and authentication port is 1812. PC is connected to Ethernet 1/16 on SWITCH1 through an unknown network. The Web server and the authentication server are connected to VLAN 1, while PC is connected to VLAN 2. 802.1x Web authentication can be enabled through the following configuration. The re-authentication function is disabled by default. To enable this, corresponding 802.1x configuration should be issued first.

Configuration task list on SWITCH1

```
Switch(config)#dot1x enable
Switch(config)#dot1x web authentication enable
Switch(config)#dot1x web redirect http://192.168.20.20/WebSupplicant/
Switch(config)#interface ethernet 1/16
Switch(Config-If-Ethernet1/16)#dot1x enable
Switch(Config-If-Ethernet1/16)#dot1x port-method webbased
```

25.4 802.1x Troubleshooting

It is possible that 802.1x be configured on ports and 802.1x authentication be set to auto, t switch can't be to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions:

- If 802.1x cannot be enabled for a port, make sure the port is not executing MAC binding, or configured as a port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.
- Web Authentication Proxy based on 802.1x is disabled by default. Open the debug dot1x switch to check debugging information when the Web Authentication Proxy based on 802.1x is opened.
- If the state display of the port is not disabled when use show dot1x, that means the Web Authentication Proxy function based on 802.1x is not close it.
- The switch of the Web Authentication Proxy based on 802.1x achieves less than 1024 users who had authenticated simultaneity on line. If exceeds this limit will return hint information.
- When the Web Authentication is failed should check whether the dot1x privateclient enable command is enabled, if the command had been enabled, then the private authentication function need close.

Chapter 26 The Number Limitation Function of Port, MAC in VLAN Configuration

26.1 Introduction to the Number Limitation Function of Port, MAC in VLAN

MAC address list is used to identify the mapping relationship between the destination MAC addresses and the ports of switch. There are two kinds of MAC addresses in the list: static MAC address and dynamic MAC address. The static MAC address is set by users, having the highest priority (will not be overwritten by dynamic MAC address), and will always be effective; dynamic MAC address is learnt by the switch through transmitting data frames, and will only be effective in a specific time range. When the switch receives a data framed waiting to be transmitted, it will study the source MAC address of the data frame, build a mapping relationship with the receiving port, and then look up the MAC address list for the destination MAC address. If any matching list entry is found, the switch will transmit the data frame via the corresponding port, or, the switch will broadcast the data frame over the VLAN it belongs to. If the dynamically learnt MAC address matches no transmitted data in a long time, the switch will delete it from the MAC address list.

Usually the switch supports both the static configuration and dynamic study of MAC address, which means each port can have more than one static set MAC addresses and dynamically learnt MAC addresses, and thus can implement the transmission of data traffic between port and known MAC addresses. When a MAC address becomes out of date, it will be dealt with broadcast. No number limitation is put on MAC address of the ports of our current switches; every port can have several MAC addressed either by configuration or study, until the hardware list entries are exhausted. To avoid too many MAC addresses of a port, we should limit the number of MAC addresses a port can have.

To summer up, it is very meaningful to develop the number limitation function of port, MAC in VLAN. Switch can control the number of MAC address of ports and VLAN through configuration commands.

Limiting the number of dynamic MAC of ports:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address of VLAN by the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function on all ports of VLAN, otherwise, the port can continue its study. (except special ports)

26.2 The Number Limitation Function of Port, MAC in VLAN Configuration Task Sequence

1. Enable the number limitation function of MAC on ports
2. Enable the number limitation function of MAC in VLAN

3. Configure the timeout value of querying dynamic MAC
4. Display and debug the relative information of number limitation of MAC on ports

1． Enable the number limitation function of MAC、IP on ports

Command	Explanation
Port configuration mode	
switchport mac-address dynamic maximum <value> **no switchport mac-address dynamic maximum**	Enable and disable the number limitation function of MAC on the ports.

2． Enable the number limitation function of MAC、IP in VLAN

Command	Explanation
VLAN configuration mode	
vlan mac-address dynamic maximum <*value*> **no vlan mac-address dynamic maximum**	Enable and disable the number limitation function of MAC in the VLAN.

3． Configure the timeout value of querying dynamic MAC.

Command	Explanation
Global configuration mode	
mac-address query timeout <*seconds*>	Configure the timeout value of querying dynamic MAC.

4．Display and debug the relative information of number limitation of MAC on ports

Command	Explanation
Admin mode	
show mac-address dynamic count {vlan <vlan-id>|interface ethernet <*portName*> }	Display the number of dynamic MAC in corresponding ports and VLAN.
debug switchport mac count **no debug switchport mac count**	All kinds of debug information when limiting the number of MAC on ports.
debug vlan mac count **no debug vlan mac count**	All kinds of debug information when limiting the number of MAC in VLAN.

26.3 The Number Limitation Function of Port, MAC in VLAN Typical Examples

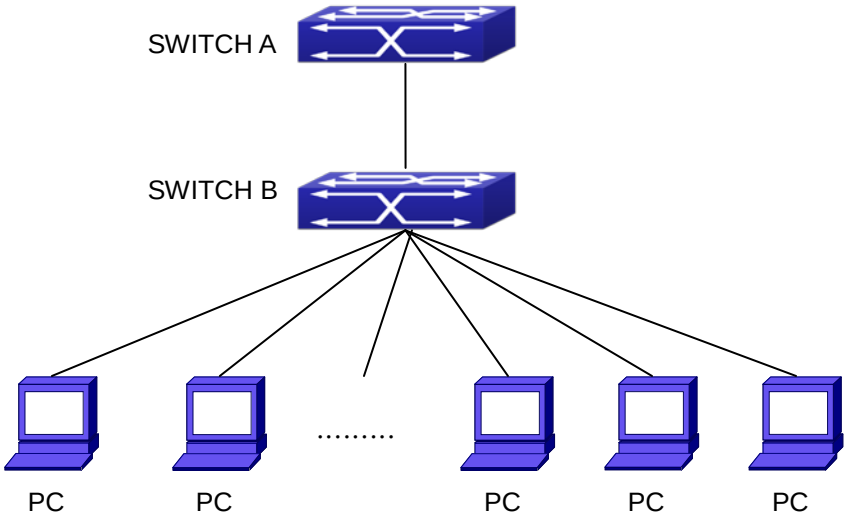


Figure 26-1 The Number Limitation of Port, MAC in VLAN Typical Configuration Example

In the network topology above, SWITCH B connects to many PC users, before enabling the number limitation function of port, MAC in VLAN, if the system hardware has no other limitation, SWTICH A and SWTICH B can get the MAC list entries of all the PC, so limiting the MAC list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC cheating, it will be easy for them to fill the MAC list entries of the switch, causing successful DOS attacks. Limiting the MAC list entry can prevent DOS attack.
On port 1/1 of SWITCH A, set the max number can be learnt of dynamic MAC address as 20. In VLAN 1, set the max number of dynamic MAC address as 30.

SWITCH A configuration task sequence:

```
Switch (config)#interface ethernet 1/1
Switch (Config-If-Ethernet1/1)#switchport mac-address dynamic maximum 20
Switch (Config-If-Ethernet1/1)#switchport arp dynamic maximum 20
Switch (Config-If-Ethernet1/1)#switchport nd dynamic maximum 10
Switch (Config-if-Vlan1)#vlan mac-address dynamic maximum 30
```

26.4 The Number Limitation Function of Port, MAC in VLAN Troubleshooting Help

The number limitation function of port, MAC in VLAN is disabled by default, if users need to limit the number of

user accessing the network, they can enable it. If the number limitation function of MAC address can not be configured, please check whether Spanning-tree, dot1x, TRUNK is running on the switch and whether the port is configured as a MAC-binding port. The number limitation function of MAC address is mutually exclusive to these configurations, so if the users need to enable the number limitation function of MAC address on the port, they should check these functions mentioned above on this port are disabled.

If all the configurations are normal, after enabling the number limitation function of port, MAC in VLAN, users can use debug commands to debug every limitation, check the details of number limitations and judge whether the number limitation function is correct. If there is any problem, please sent result to technical service center.

Chapter 27 Operational Configuration of AM Function

27.1 Introduction to AM Function

AM (Access Management) means that when a switch receives an IP or ARP message, it will compare the information extracted from the message (such as source IP address or source MAC-IP address) with the configured hardware address pool. If there is an entry in the address pool matching the information (source IP address or source MAC-IP address), the message will be forwarded, otherwise, dumped. The reason why source-IP-based AM should be supplemented by source-MAC-IP-based AM is that IP address of a host might change. Only with a bound IP, can users change the IP of the host into forwarding IP, and hence enable the messages from the host to be forwarded by the switch. Given the fact that MAC-IP can be exclusively bound with a host, it is necessary to make MAC-IP bound with a host for the purpose of preventing users from maliciously modifying host IP to forward the messages from their hosts via the switch.

With the interface-bound attribute of AM, network mangers can bind the IP (MAC-IP) address of a legal user to a specified interface. After that, only the messages sending by users with specified IP (MAC-IP) addresses can be forwarded via the interface, and thus strengthen the monitoring of the network security.

27.2 AM Function Configuration Task List

1 · Enable AM function
2 · Enable AM function on an interface
3 · Configure the forwarding IP
4 · Configure the forwarding MAC-IP
5 · Delete all of the configured IP or MAC-IP or both
6 · Display relative configuration information of AM

1. Enable AM function

Command	Explanation
Global Mode	
am enable **no am enable**	Globally enable or disable AM function.

2. Enable AM function on an interface

Command	Explanation
Port Mode	

am port **no am port**	Enable/disable AM function on the port. When the AM function is enabled on the port, no IP or ARP message will be forwarded by default.

3. Configure the forwarding IP

Command	Explanation
Port Mode	
am ip-pool <*ip-address*> <*num*> **no am ip-pool <*ip-address*> <*num*>**	Configure the forwarding IP of the port.

4. Configure the forwarding MAC-IP

Command	Explanation
Port Mode	
am mac-ip-pool <*mac-address*> <*ip-address*> **no am mac-ip-pool <*mac-address*> <*ip-address*>**	Configure the forwarding MAC-IP of the port.

5. Delete all of the configured IP or MAC-IP or both

Command	Explanation
Global Mode	
no am all [ip-pool|mac-ip-pool]	Delete MAC-IP address pool or IP address pool or both pools configured by all users.

6. Display relative configuration information of AM

Command	Explanation
Global Configuration Mode	
show am [interface <*interface-name*>]	Display the AM configuration information of one port or all ports.

27.3 AM Function Example

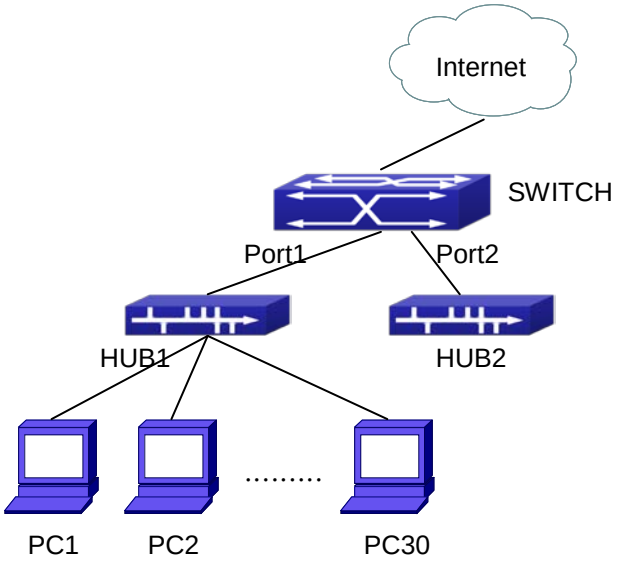


Figure 27-1 a typical configuration example of AM function

In the topology above, 30 PCs, after converged by HUB1, connect with interface1 on the switch. The IP addresses of these 30 PCs range from 100.10.10.1 to 100.10.10.30. Considering security, the system manager will only take user with an IP address within that range as legal ones. And the switch will only forward data packets from legal users while dumping packets from other users.

According to the requirements mentioned above, the switch can be configured as follows:

```
Switch(config)#am enable
Switch(config)#interface ethernet1/1
Switch(Config-If-Ethernet1/1)#am port
Switch(Config-If-Ethernet1/1)#am ip-pool 10.10.10.1 10
```

27.4 AM Function Troubleshooting

AM function is disabled by default, and after it is enabled, relative configuration of AM can be made.

Users can view the current AM configuration with “show am” command, such as whether the AM is enabled or not, and AM information on each interface, they can also use “**show am [interface *<interface-name>*]**” command to check the AM configuration information on a specific interface.

If any operational error happens, the system will display detailed corresponding prompt.

Chapter 28 Security Feature Configuration

28.1 Introduction to Security Feature

Before introducing the security features, we here first introduce the DoS. The DoS is short for Denial of Service, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

28.2 Security Feature Configuration

28.2.1 Prevent IP Spoofing Function Configuration Task Sequence

1 · Enable the IP spoofing function.

Command	Explanation
Global Mode	
[no] dosattack-check srcip-equal-dstip enable	Enable/disable the function of checking if the IP source address is the same as the destination address.

28.2.2 Prevent TCP Unauthorized Label Attack Function Configuration Task Sequence

1 · Enable the anti TCP unauthorized label attack function

2 · Enable Checking IPv4 fragment function

Command	Explanation
Global Mode	
[no] dosattack-check tcp-flags enable	Enable/disable checking TCP label function

[no] dosattack-check ipv4-first-fragment enable	Enable/disable checking IPv4 fragment. This command has no effect when used separately, but if this function is not enabled, the switch will not drop the IPv4 fragment packet containing unauthorized TCP labels.

28.2.3 Anti Port Cheat Function Configuration Task Sequence

1 · Enable the anti port cheat function

Command	Explanation
Global Mode	
[no] dosattack-check srcport-equal-dstport enable	Enable/disable the prevent-port-cheat function.
dosattack-check ipv4-first-fragment enable	Enable/disable checking IPv4 fragment. This command has no effect when used separately, but if this function is not enabled, the switch will not drop the IPv4 fragment packet whose source port is equal to its destination port.

28.2.4 Prevent TCP Fragment Attack Function Configuration Task Sequence

1 · Enable the prevent TCP fragment attack function

2 · Configure the minimum permitted TCP head length of the packet

Command	Explanation
Global Mode	
[no] dosattack-check tcp-fragment enable	Enable/disable the prevent TCP fragment attack function.
dosattack-check tcp-header <*size*>	Configure the minimum permitted TCP head length of the packet. This command has no effect when used separately, the user should enable the **dosattack-check tcp-fragment enable**.

28.2.5 Prevent ICMP Fragment Attack Function Configuration Task Sequence

1. Enable the prevent ICMP fragment attack function
2. Configure the max permitted ICMPv4 net load length
3. Configure the max permitted ICMPv6 net load length

Command	Explanation
Global Mode	
[no] dosattack-check icmp-attacking enable	Enable/disable the prevent ICMP fragment attack function.
dosattack-check icmpv4-size <*size*>	Configure the max permitted ICMPv4 net load length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable.**
dosattack-check icmpv6-size <*size*>	Configure the max permitted ICMPv6 net load length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable.**

28.3 Security Feature Example

Scenario:

The User has follows configuration requirements: the switch do not forward data packet whose source IP address is equal to the destination address, and those whose source port is equal to the destination port. Only the ping command with defaulted options is allowed within the IPv4 network, namely the ICMP request packet can not be fragmented and its net length is normally smaller than 100.

Configuration procedure:

```
Switch(config)# dosattack-check srcip-equal-dstip enable
Switch(config)# dosattack-check srcport-equal-dstport enable
Switch(config)# dosattack-check ipv4-first-fragment enable
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpV4-size 100
```

Chapter 29 TACACS+ Configuration

29.1 Introduction to TACACS+

TACACS+ terminal access controller access control protocol is a protocol similar to the radius protocol for control the terminal access to the network. Three independent functions of Authentication, Authorization, Accounting are also available in this protocol. Compared with RADIUS, the transmission layer of TACACS+ protocol is adopted with TCP protocol, further with the packet head (except for standard packet head) encryption, this protocol is of a more reliable transmission and encryption characteristics, and is more adapted to security control.

According to the characteristics of the TACACS+ (Version 1.78), we provide TACACS+ authentication function on the switch, when the user logs, such as telnet, the authentication of user name and password can be carried out with TACACS+.

29.2 TACACS+ Configuration Task List

1. Configure the TACACS+ authentication key
2. Configure the TACACS+ server
3. Configure the TACACS+ authentication timeout time
4. Configure the IP address of the RADIUS NAS

1. Configure the TACACS+ authentication key

Command	Explanation
Global Mode	
tacacs-server key <*string*> **no tacacs-server key**	Configure the TACACS+ server key; the "**no tacacs-server key**" command deletes the key.

2. Configure TACACS+ server

Command	Explanation
Global Mode	
tacacs-server authentication host <*IPaddress*> [[port {<*portNum*>}] [timeout <*seconds*>] [key <string>] [primary]] **no tacacs-server authentication host <*IPaddress*>**	Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the no form of this command deletes the TACACS+ authentication server.

3. Configure the TACACS+ authentication timeout time

Command	Explanation
Global Mode	
tacacs-server timeout <*seconds*> **no tacacs-server timeout**	Configure the authentication timeout for the TACACS+ server, the "**no tacacs-server timeout**" command restores the default configuration.

4. Configure the IP address of the TACACS+ NAS

Command	Explanation
Global Mode	
tacacs-server nas-ipv4 <*ip-address*> **no tacacs-server nas-ipv4**	To configure the source IP address for the TACACS+ packets for the switch.

29.3 TACACS+ Scenarios Typical Examples

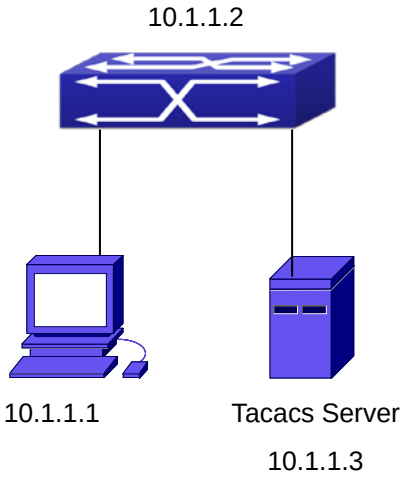


Figure 29-1 TACACS Configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a TACACS+ authentication server; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 49, set telnet log on authentication of the switch as tacacs local, via using TACACS+ authentication server to achieve telnet user authentication.

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#tacacs-server authentication host 10.1.1.3
```

```
Switch(config)#tacacs-server key test
Switch(config)#authentication login vty tacacs local
```

29.4 TACACS+ Troubleshooting

In configuring and using TACACS+, the TACACS+ may fail to authentication due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- First good condition of the TACACS+ server physical connection.
- Second all interface and link protocols are in the UP state (use "**show interface**" command).
- Then ensure the TACACS+ key configured on the switch is in accordance with the one configured on TACACS+ server.
- Finally ensure to connect to the correct TACACS+ server.

Chapter 30 RADIUS Configuration

30.1 Introduction to RADIUS

30.1.1 AAA and RADIUS Introduction

AAA is short for Authentication, Authorization and Accounting, it provide a consistency framework for the network management safely. According to the three functions of Authentication, Authorization, Accounting, the framework can meet the access control for the security network: which one can visit the network device, which access-level the user can have and the accounting for the network resource.

RADIUS (Remote Authentication Dial in User Service), is a kind of distributed and client/server protocol for information exchange. The RADIUS client is usually used on network appliance to implement AAA in cooperation with 802.1x protocol. The RADIUS server maintains the database for AAA, and communicates with the RADIUS client through RADIUS protocol. The RADIUS protocol is the most common used protocol in the AAA framework.

30.1.2 Message structure for RADIUS

The RADIUS protocol uses UDP to deliver protocol packets. The packet format is shown as below.

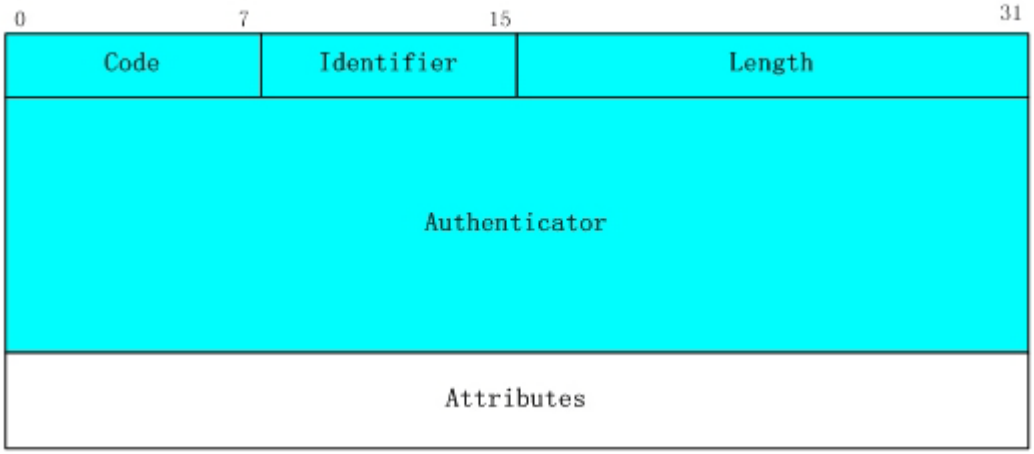


Figure 30-1 Message structure for RADIUS

Code field(1octets): is the type of the RADIUS packet. Available value for the Code field is show as below:

1 · Access-Request
2 · Access-Accept
3 · Access-Reject
4 · Accounting-Request
5 · Accounting-Response
6 · Access-Challenge

Identifier field (1 octet): Identifier for the request and answer packets.
Length field (2 octets): The length of the overall RADIUS packet, including Code, Identifier, Length, Authenticator and Attributes

Authenticator field (16 octets): used for validation of the packets received from the RADIUS server. Or it can be used to carry encrypted passwords. This field falls into two kinds: the Request Authenticator and the Response Authenticator.

Attribute field: used to carry detailed information about AAA. An Attribute value is formed by Type, Length, and Value fields.

- Type field (1 octet), the type of the attribute value, which is shown as below:

Property	Type of property	Property	Type of property
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

- Length field (1 octet), the length in octets of the attribute including Type, Length and Value fields.
- Value field, value of the attribute whose content and format is determined by the type and length of the attribute.

30.2 RADIUS Configuration Task List

1 · Enable the authentication and accounting function.
2 · Configure the RADIUS authentication key.
3 · Configure the RADIUS server.
4 · Configure the parameter of the RADIUS service.
5 · Configure the IP address of the RADIUS NAS.

1. Enable the authentication and accounting function.

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	To enable the AAA authentication function. The no form of this command will disable the AAA authentication function.
aaa-accounting enable **no aaa-accounting enable**	To enable AAA accounting. The no form of this command will disable AAA accounting.
aaa-accounting update {enable|disable}	Enable or disable the update accounting function.

2. Configure the RADIUS authentication key.

Command	Explanation
Global Mode	
radius-server key <*string*> **no radius-server key**	To configure the encryption key for the RADIUS server. The no form of this command will remove the configured key.

3. Configure the RADIUS server.

Command	Explanation
Global Mode	
radius-server authentication host { ***<IPaddress>*** **|** ***<IPv6address>*** **} [[port {*<portNum>*}] [key *<string>]* [primary] [access-mode {dot1x|telnet}]** **no radius-server authentication host *<IPaddress>***	Specifies the IP address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no command deletes the RADIUS authentication server.
radius-server accounting host { *<IPaddress>* | *<IPv6address>* } [[port {*<portNum>*}] [primary]] **no radius-server accounting host *<IPaddress>***	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

4. Configure the parameter of the RADIUS service

Command	Explanation
Global Mode	
radius-server dead-time <*minutes*> **no radius-server dead-time**	To configure the interval that the RADIUS becomes available after it is down. The no form of this command will restore the default configuration.
radius-server retransmit <*retries*> **no radius-server retransmit**	To configure retry times for the RADIUS packets. The no form of this command restores the default configuration.
radius-server timeout <*seconds*> **no radius-server timeout**	To configure the timeout value for the RADIUS server. The no form of this command will restore the default configuration.
radius-server accounting-interim-update timeout <*seconds*> **no radius-server accounting-interim-update timeout**	To configure the update interval for accounting. The no form of this command will restore the default configuration.

5. Configure the IP address of the RADIUS NAS

Command	Explanation
Global Mode	
radius nas-ipv4 <*ip-address*> **no radius nas-ipv4**	To configure the source IP address for the RADIUS packets for the switch.
radius nas-ipv6 <*ipv6-address*> **no radius nas-ipv6**	To configure the source IPv6 address for the RADIUS packets for the switch.

30.3 RADIUS Typical Examples

30.3.1 IPv4 Radius Example

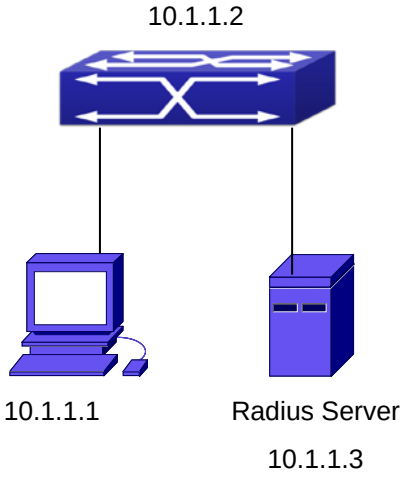


Figure 30-2 The Topology of IEEE802.1x configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a RADIUS authentication server without Ethernet1/2; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.

Configure steps as below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

30.3.2 IPv6 RadiusExample

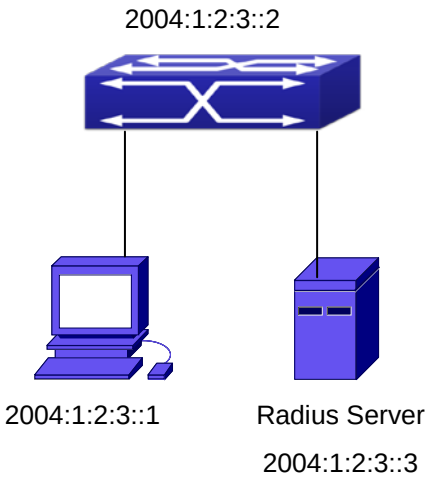


Figure 30-3 The Topology of IPv6 Radius configuration

A computer connects to a switch, of which the IP address is 2004:1:2:3::2 and connected with a RADIUS authentication server without Ethernet1/2; IP address of the server is 2004:1:2:3::3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.
Configure steps as below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

30.4 RADIUS Troubleshooting

In configuring and using RADIUS, the RADIUS may fail to authentication due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- First make sure good condition of the RADIUS server physical connection;
- Second all interface and link protocols are in the UP state (use "**show interface**" command)
- Then ensure the RADIUS key configured on the switch is in accordance with the one configured on RADIUS server;
- Finally ensure to connect to the correct RADIUS server

If the RADIUS authentication problem remains unsolved, please use **debug aaa** and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical

server center of our company.

Chapter 31 MRPP Configuration

31.1 Introduction to MRPP

MRPP (Multi-layer Ring Protection Protocol), is a link layer protocol applied on Ethernet loop protection. It can avoid broadcast storm caused by data loop on Ethernet ring, and restore communication among every node on ring network when the Ethernet ring has a break link. MRPP is the expansion of EAPS (Ethernet link automatic protection protocol).

MRPP protocol is similar to STP protocol on function, MRPP has below characters, compare to STP protocol:

<1> MRPP specifically uses to Ethernet ring topology

<2> fast convergence, less than 1 s. ideally it can reach 100-50 ms.

31.1.1 Conception Introduction

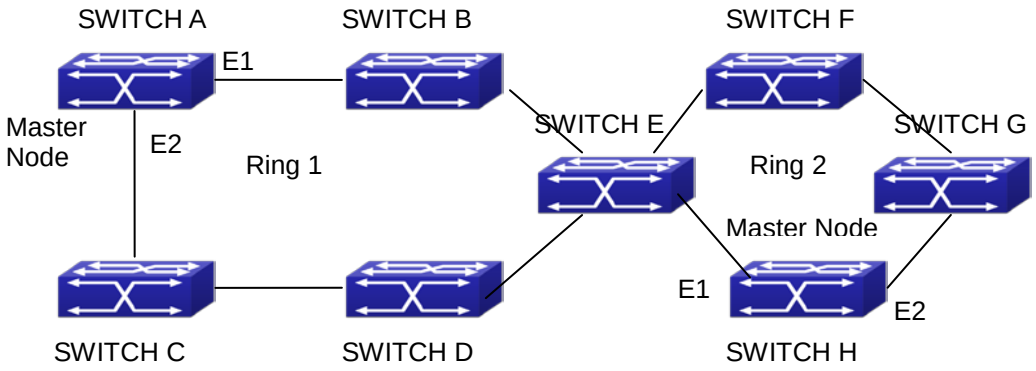


Figure 31-1 MRPP Sketch Map

1. Control VLAN

Control VLAN is a virtual VLAN, only used to identify MRPP protocol packet transferred in the link. To avoid confusion with other configured VLAN, avoids configuring control VLAN ID to be the same with other configured VLAN ID. The different MRPP ring should configure the different control VLAN ID.

2. Ethernet Ring (MRPP Ring)

Ring linked Ethernet network topology.

Each MRPP ring has two states.

Health state: The whole ring net work physical link is connected.

Break state: one or a few physical link break in ring network

3. nodes

Each switch is named after a node on Ethernet. The node has some types:

Primary node: each ring has a primary node, it is main node to detect and defend.

Transfer node: except for primary node, other nodes are transfer nodes on each ring.

The node role is determined by user configuration. As shown Fig 31-1, Switch A is primary node of Ring 1, Switch B. Switch C; Switch D and Switch E are transfer nodes of Ring 1.

4. Primary port and secondary port

The primary node and transfer node have two ports connecting to Ethernet separately, one is primary port, and another is secondary port. The role of port is determined by user configuration.

Primary port and secondary port of primary node

The primary port of primary node is used to send ring health examine packet (hello), the secondary port is used to receive Hello packet sending from primary node. When the Ethernet is in health state, the secondary port of primary node blocks other data in logical and only MRPP packet can pass. When the Ethernet is in break state, the secondary port of primary node releases block state, and forwards data packets.

There are no difference on function between Primary port and secondary port of transfer node.

The role of port is determined by user configuration. As shown Fig 31-1, Switch A E1 is primary port, E2 is secondary port.

5. Timer

The two timers are used when the primary node sends and receives MRPP protocol packet: Hello timer and Fail Timer.

Hello timer: define timer of time interval of health examine packet sending by primary node primary port.

Fail timer: define timer of overtime interval of health examine packet receiving by primary node primary port.

The value of Fail timer must be more than or equal to the 3 times of value of Hello timer.

31.1.2 MRPP Protocol Packet Types

Packet Type	Explanation
Hello packet (Health examine packet) Hello	The primary port of primary node evokes to detect ring, if the secondary port of primary node can receive Hello packet in configured overtime, so the ring is normal.
LINK-DOWN (link Down event packet)	After transfer node detects Down event on port, immediately sends LINK-DOWN packet to primary node, and inform primary node ring to fail.
LINK-DOWN-FLUSH_FDB packet	After primary node detects ring failure or receives LINK-DOWN packet, open blocked secondary port, and then uses two ports to send the packet, to inform each transfer node to refresh own MAC address.
LINK-UP-FLUSH_FDB packet	After primary detects ring failure to restore normal, and uses packet from primary port, and informs each transfer node to refresh own MAC address.

31.1.3 MRPP Protocol Operation System

1. Link Down Alarm System

When transfer node finds themselves belonging to MRPP ring port Down, it sends link Down packet to primary node immediately. The primary node receives link down packet and immediately releases block state of secondary port, and sends LINK-DOWN-FLUSH-FDB packet to inform all of transfer nodes, refreshing own MAC address forward list.

2. Poll System

The primary port of primary node sends Hello packet to its neighbors timely according to configured Hello-timer.

If the ring is health, the secondary port of primary node receives health detect packet, and the primary node keeps secondary port.

If the ring is break, the secondary port of primary node can't receive health detect packet when timer is over time. The primary releases the secondary port block state, and sends LINK-DOWN-FLUSH_FDB packet to inform all of transfer nodes, to refresh own MAC address forward list.

3. Ring Restore

After the primary node occur ring fail, if the secondary port receives Hello packet sending from primary node, the ring has been restored, at the same time the primary node block its secondary port, and sends its neighbor LINK-UP-Flush-FDB packet.

After MRPP ring port refresh UP on transfer node, the primary node maybe find ring restore after a while. For the normal data VLAN, the network maybe forms a temporary ring and creates broadcast storm. To avoid temporary ring, transfer node finds it to connect to ring network port to refresh UP, immediately block temporarily (only permit control VLAN packet pass), after only receiving LINK-UP-FLUSH-FDB packet from primary node, and releases the port block state.

31.2 MRPP Configuration Task List

1) Globally enable MRPP
2) Configure MRPP ring
3) Display and debug MRPP relevant information

1) Globally enable MRPP

Command	Explanation
Global Mode	
mrpp enable **no mrpp enable**	Globally enable and disable MRPP.

2) Configure MRPP ring

Command	Explanation
Global Mode	
mrpp ring <*ring-id*> **no mrpp ring <*ring-id*>**	Create MRPP ring. The “no” command deletes MRPP ring and its configuration.
MRPP ring mode	
control-vlan <*vid*> **no control-vlan**	Configure control VLAN ID, format “no” deletes configured control VLAN ID.
node-mode {master | transit}	Configure node type of MRPP ring (primary node or secondary node).
hello-timer < *timer*> **no hello-timer**	Configure Hello packet timer sending from primary node of MRPP ring, format “no” restores default timer value.
fail-timer <*timer*> **no fail-timer**	Configure Hello packet overtime timer sending from primary node of MRPP ring, format “no” restores default timer value.
enable **no enable**	Enable MRPP ring, format “no” disables enabled MRPP ring.
Port mode	
mrpp ring <*ring-id*> primary-port **no mrpp ring <*ring-id*> primary-port**	Specify primary port of MRPP ring.
mrpp ring <*ring-id*> secondary-port **no mrpp ring <*ring-id*> secondary-port**	Specify secondary port of MRPP ring.

3) Display and debug MRPP relevant information

Command	Explanation
Admin Mode	
debug mrpp **no debug mrpp**	Disable MRPP module debug information, format “no” disable MRPP debug information output.
show mrpp {<*ring-id*>}	Display MRPP ring configuration information.
show mrpp statistics {<*ring-id*>}	Display receiving data packet statistic information of MRPP ring.
clear mrpp statistics {<*ring-id*>}	Clear receiving data packet statistic information of MRPP ring.

31.3 MRPP Typical Scenario

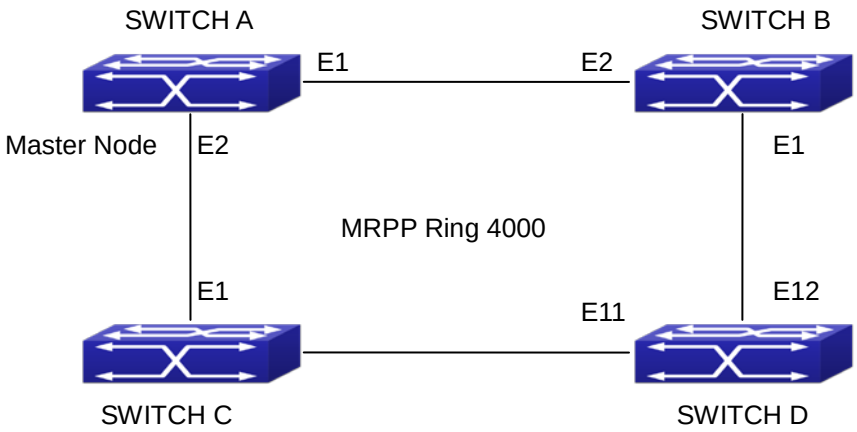


Figure 31-2 MRPP typical configuration scenario

The above topology often occurs on using MRPP protocol. The multi switch constitutes a single MRPP ring, all of the switches only are configured an MRPP ring 4000, thereby constitutes a single MRPP ring.

In above configuration, SWITCH A configuration is primary node of MRPP ring 4000, and configures E1/1 to primary port, E1/2 to secondary port. Other switches are secondary nodes of MRPP ring, configures primary port and secondary port separately.

To avoid ring, it should temporarily disable one of the ports of primary node, when it enables each MRPP ring in the whole MRPP ring; and after all of the nodes are configured, open the port.

When disable MRPP ring, it needs to insure the MRPP ring doesn't have ring.

SWITCH A configuration Task Sequence:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 5
Switch(mrpp-ring-4000)#node-mode master
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH B configuration Task Sequence:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH C configuration Task Sequence:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

SWITCH D configuration Task Sequence:

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/1
Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/1)#interface ethernet 1/2
Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/2)#exit
Switch(Config)#
```

31.4 MRPP Troubleshooting

The normal operation of MRPP protocol depends on normal configuration of each switch on MRPP ring, otherwise it is very possible to form ring and broadcast storm:

- Configuring MRPP ring, you'd better disconnected the ring, and wait for each switch configuration, then open the ring.
- When the MRPP ring of enabled switch is disabled on MRPP ring, it ensures the ring of the MRPP ring has been disconnected.
- When there is broadcast storm on MRPP ring, it disconnects the ring firstly, and ensures if each switch MRPP ring configuration on the ring is correct or not; if correct, restores the ring, and then observes the ring is normal or not.
- In normal configuration, it still forms ring broadcast storm or ring block, please open debug function of primary node MRPP, and used show MRPP statistics command to observe states of primary node and transfer node and statistics information is normal or not, and then sends results to our Technology Service Center.

Chapter 32 Mirror Configuration

32.1 Introduction to Mirror

Mirror functions include port mirror function, CPU mirror function, flow mirror function.

Port mirror refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as mirror destination port. A protocol analyzer (such as Sniffer) or a RMON monitor will be connected at mirror destination port to monitor and manage the network, and diagnose the problems in the network.

CPU mirror function means that the switch exactly copies the data frames received or sent by the CPU to a port.

Flow mirror function means that the switch exactly copies the data frames received or by the specified rule of a port to another port. The flow mirror will take effect only the specified rule is permit.

A chassis switch supports at most 4 mirror destination ports, each boardcard allows a source or destination port of a mirror session. At present, each box switch can set many mirror sessions.There is no limitation on mirror source ports, one port or several ports is allowed. When there are more than one source ports, they can be in the same VLAN or in different VLAN. The source port and destination port can be in different VLAN.

32.2 Mirror Configuration Task List

1) Specify mirror destination port
2) Specify mirror source port（CPU）
3) Specify flow mirror source

1. Specify mirror destination port

Command	Explanation
Global Mode	
monitor session <*session*> destination interface <*interface-number*> **no monitor session <*session*> destination interface <*interface-number*>**	Specifies mirror destination port; the no command deletes mirror destination source port.

2. Specify mirror source port （CPU）

Command	Explanation
Global Mode	

monitor session <*session*> source {interface <*interface-list*> | cpu} {rx| tx| both} **no monitor session <*session*> source {interface <*interface-list*> | cpu}**	Specifies mirror source port; the no command deletes mirror source port.

3. Specify flow mirror source

Command	Explanation
Global Mode	
monitor session <*session*> source {interface <*interface-list*>} access-group <*num*> {rx|tx|both} **no monitor session <*session*> source {interface <*interface-list*>} access-group <*num*>**	Specifies flow mirror source port and apply rule; the no command deletes flow mirror source port.

32.3 Mirror Examples

The requirement of the configurations is shown as below: to monitor at interface 1 the data frames sent out by interface 9 and received from interface 7, sent and received by CPU, and the data frames received by interface 15 and matched by rule 120(The source IP address is 1.2.3.4 and the destination IP address is 5.6.7.8).

Configuration guidelines:

1. Configure interface 1 to be a mirror destination interface.
2. Configure the interface 7 ingress and interface 9 egress to be mirrored source.
3. Configure the CPU as one of the source.
4. Configure access list 120.
5. Configure access 120 to binding interface 15 ingress.

Configuration procedure is as follows:

```
Switch(config)#monitor session 4 destination interface ethernet 1/1
Switch(config)#monitor session 4 source interface ethernet 1/7 rx
Switch(config)#monitor session 4 source interface ethernet 1/9 tx
Switch(config)#monitor session 4 source cpu
Switch(config)#access-list 120 permit tcp 1.2.3.4 0.0.0.255 5.6.7.8 0.0.0.255
Switch(config)#monitor session 4 source interface ethernet 1/15 access-list 120 rx
```

32.4 Device Mirror Troubleshooting

If problems occur on configuring port mirroring, please check the following first for causes:

- Whether the mirror destination port is a member of a TRUNK group or not, if yes, modify the TRUNK group.
- If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port. Mirror destination port can not be pulled into Isolate vlan, or will affect mirror between VLAN.

Chapter 33 sFlow Configuration

33.1 Introduction to sFlow

The sFlow (RFC 3176) is a protocol based on standard network export and used on monitoring the network traffic information developed by the InMon Company. The monitored switch or router sends date to the client analyzer through its main operations such as sampling and statistic, then the analyzer will analyze according to the user requirements so to monitor the network.

A sFlow monitor system includes: sFlow proxy, central data collector and sFlow analyzer. The sFlow proxy collects data from the switch using sampling technology. The sFlow collector is for formatting the sample data statistic which is to be forwarded to the sFlow analyzer which will analyze the sample data and perform corresponding measure according to the result. Our switch here acts as the proxy and central data collector in the sFlow system.

We have achieved data sampling and statistic targeting physical port.

Our data sample includes the IPv4 and IPv6 packets. Extensions of other types are not supported so far. As for non IPv4 and IPv6 packet, the unify HEADER mode will be adopted following the requirements in RFC3176, copying the head information of the packet based on analyzing the type of its protocol.

The latest sFlow protocol presented by InMon Company is the version 5. Since it is the version 4 which is realized in the RFC3176, version conflict might exist in some case such as the structure and the packet format. This is because the version 5 has not become the official protocol, so, in order to be compatible with current applications, we will continue to follow the RFC3176.

33.2 sFlow Configuration Task List

1. Configure sFlow Collector address

Command	Explanation
Global mode and Port Mode	
sflow destination <*collector-address*> **[<*collector-port*>]** **no sflow destination**	Configure the IP address and port number of the host in which the sFlow analysis software is installed. As for the ports, if IP address is configured on the port, the port configuration will be applied, or else will be applied the global configuration. The "**no sflow destination**" command restores to the default port value and deletes the IP address.

2. Configure the sFlow proxy address

Command	Explanation
Global Mode	
sflow agent-address <*collector-address*> **no sflow agent-address**	Configure the source IP address applied by the sFlow proxy; the “no” form of the command deletes this address.

3. Configure the sFlow proxy priority

Command	Explanation
Global Mode	
sflow priority <*priority-vlaue*> **no sflow priority**	Configure the priority when sFlow receives packet from the hardware; the “**no sflow priority**” command restores to the default

4. Configure the packet head length copied by sFlow

Command	Explanation
Port Mode	
sflow header-len <*length-vlaue*> **no sflow header-len**	Configure the length of the packet data head copied in the sFlow data sampling; the “no” form of this command restores to the default value.

5. Configure the max data head length of the sFlow packet

Command	Explanation
Port Mode	
sflow data-len <*length-vlaue*> **no sflow data-len**	Configure the max length of the data packet in sFlow; the “no” form of this command restores to the default.

6. Configure the sampling rate value

Command	Explanation
Port Mode	
sflow rate {input <*input-rate*> | **output <*output-rate* >}** **no sflow rate [input | output]**	Configure the sampling rate when sFlow performing hardware sampling. The “no” command deletes the rate value.

7. Configure the sFlow statistic sampling interval

Command	Explanation

Port Mode	
sflow counter-interval <*interval-vlaue*> **no sflow counter-interval**	Configure the max interval when sFlow performing statistic sampling. The “no” form of this command deletes

33.3 sFlow Examples

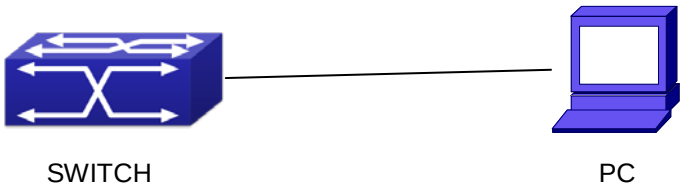


Figure 33-1 sFlow configuration topology

As shown in the figure, sFlow sampling is enabled on the port 1/1 and 1/2 of the switch. Assume the sFlow analysis software is installed on the PC with the address of 192.168.1.200. The address of the layer 3 interface on the SwitchA connected with PC is 192.168.1.100. A loopback interface with the address of 10.1.144.2 is configured on the SwitchA. sFlow configuration is as follows:

Configuration procedure is as follows:

```
Switch#config
Switch (config)#sflow ageng-address 10.1.144.2
Switch (config)#sflow destination 192.168.1.200
Switch (config)#sflow priority 1
Switch (config)# interface ethernet1/1
Switch (Config-If-Ethernet1/1)#sflow rate input 10000
Switch (Config-If-Ethernet1/1)#sflow rate output 10000
Switch (Config-If-Ethernet1/1)#sflow counter-interval 20
Switch (Config-If-Ethernet1/1)#exit
Switch (config)# interface ethernet1/2
Switch (Config-If-Ethernet1/2)#sflow rate input 20000
Switch (Config-If-Ethernet1/2)#sflow rate output 20000
Switch (Config-If-Ethernet1/2)#sflow counter-interval 40
```

33.4 sFlow Troubleshooting

In configuring and using sFlow, the sFlow server may fail to run properly due to physical connection failure,

wrong configuration, etc. The user should ensure the following:

- Ensure the physical connection is correct
- Guarantee the address of the sFlow analyzer configured under global or port mode is accessible.
- If traffic sampling is required, the sampling rate of the interface must be configured
- If statistic sampling is required, the statistic sampling interval of the interface must be configured

If the examination remains unsolved, please contact with the technical service center of our company.

Chapter 34 SNTP Configuration

34.1 Introduction to SNTP

The Network Time Protocol (NTP) is widely used for clock synchronization for global computers connected to the Internet. NTP can assess packet sending/receiving delay in the network, and estimate the computer's clock deviation independently, so as to achieve high accuracy in network computer clocking. In most positions, NTP can provide accuracy from 1 to 50ms according to the characteristics of the synchronization source and network route.

Simple Network Time Protocol (SNTP) is the simplified version of NTP, removing the complex algorithm of NTP. SNTP is used for hosts who do not require full NTP functions; it is a subset of NTP. It is common practice to synchronize the clocks of several hosts in local area network with other NTP hosts through the Internet, and use those hosts to provide time synchronization service for other clients in LAN. The figure below depicts a NTP/SNTP application network topology, where SNTP mainly works between second level servers and various terminals since such scenarios do not require very high time accuracy, and the accuracy of SNTP (1 to 50 ms) is usually sufficient for those services.

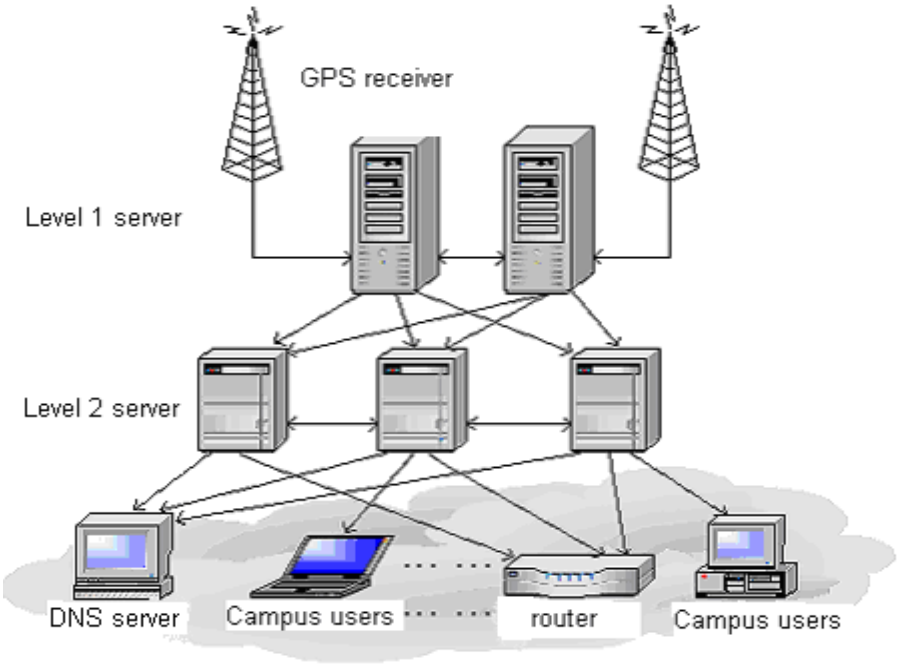


Figure 34-1 Working Scenario

Switch implements SNTPv4 and supports SNTP client unicast as described in RFC2030; SNTP client multicast and unicast are not supported, nor is the SNTP server function.

34.2 Typical Examples of SNTP Configuration

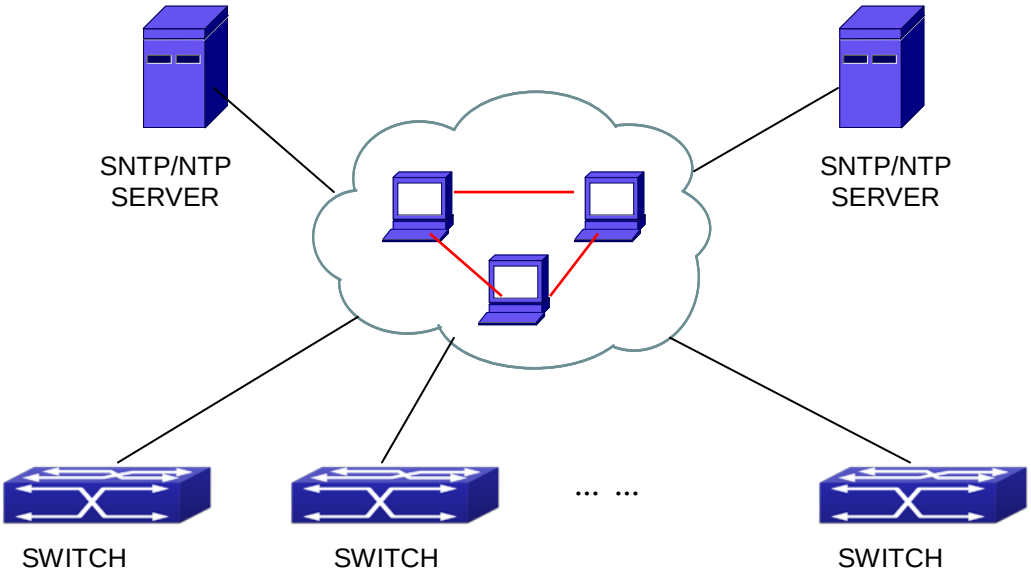


Figure 34-2 Typical SNTP Configuration

All switches in the autonomous zone are required to perform time synchronization, which is done through two redundant SNTP/NTP servers. For time to be synchronized, the network must be properly configured. There should be reachable route between any switch and the two SNTP/NTP servers.

Example: Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1, respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any switch should like the following:

```
Switch#config
Switch(config)#sntp server 10.1.1.1
```

Chapter 35 Monitor and Debug

When the users configures the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in network failure, the users will also need to diagnostic the problem. Switch provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

35.1 Ping

Ping command is mainly used for sending ICMP query packet from the switches to remote devices, also for check the accessibility between the switch and the remote device. Refer to the Ping command chapter in the Command Manual for explanations of various parameters and options of the Ping command.

35.2 Ping6

Ping6 command is mainly used by the switch to send ICMPv6 query packet to the remote equipment, verifying the accessibility between the switch and the remote equipment. Options and explanations of the parameters of the Ping6 command please refer to Ping6 command chapter in the command manual.

35.3 Traceroute

Traceroute command is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.
Execution procedure of the Traceroute command consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination.
Traceroute Options and explanations of the parameters of the Traceroute command please refer to traceroute command chapter in the command manual.

35.4 Traceroute6

The Traceroute6 function is used on testing the gateways passed through by the data packets from the source equipment to the destination equipment, to verify the accessibility and locate the network failure. The principle

of the Traceroute6 under IPv6 is the same as that under IPv4, which adopts the hop limit field of the ICMPv6 and IPv6 header. First, Traceroute6 sends an IPv6 datagram (including source address, destination address and packet sent time) whose HOPLIMIT is set to 1. When first route on the path receives this datagram, it minus the HOPLIMIT by 1 and the HOPLIMIT is now 0. So the router will discard this datagram and returns with a「ICMPv6 time exceeded」message (including the source address of the IPv6 packet, all content in the IPv6 packet and the IPv6 address of the router). Upon receiving this message, the Traceroute6 sends another datagram of which the HOPLIMIT is increased to 2 so to discover the second router. Plus 1 to the HOPLIMIT every time to discover another router, the Traceroute6 repeat this action till certain datagram reaches the destination.

Traceroute6 Options and explanations of the parameters of the Traceroute6 command please refer to traceroute6 command chapter in the command manual.

35.5 Show

show command is used to display information about the system , port and protocol operation. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

Admin Mode	
show debugging	Display the debugging state.
show flash	Display the files and the sizes saved in the flash.
show history	Display the recent user input history command.
show memory	Display content in specified memory area.
show running-config	Display the switch parameter configuration validating at current operation state.
show startup-config	Display the switch parameter configuration written in the Flash Memory at current operation state, which is normally the configuration file applied in next time the switch starts up.
show switchport interface [ethernet *<IFNAME>*]	Display the VLAN port mode and the belonging VLAN number of the switch as well as the Trunk port information.
show tcp	Display the TCP connection status established currently on the switch.
show udp	Display the UDP connection status established currently on the switch.
show telnet login	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

show tech-support	Display the operation information and the state of each task running on the switch. It is used by the technicians to diagnose whether the switch operates properly.
show version	Display the version of the switch.
show temperature	Show CPU temperature of the switch.

35.6 Debug

All the protocols switch supports have their corresponding debug commands. The users can use the information from debug commands for troubleshooting. Debug commands for their corresponding protocols will be introduced in the later chapters.

35.7 System log

35.7.1 System Log Introduction

The system log takes all information output under it control, while making detailed catalogue, so to select the information effectively. Combining with Debug programs, it will provide a powerful support to the network administrator and developer in monitoring the network operation state and locating the network failures.

The switch system log has following characteristics

- Log output from four directions (or log channels) of the Console, Telnet terminal and monitor, log buffer zone, and log host.
- The log information is classified to four level of severities by which the information will be filtered
- According to the severity level the log information can be auto outputted to corresponding log channel.

35.7.1.1 Log Output Channel

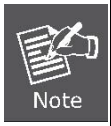
So far the system log can be outputted the log information through four channels:

- Through Console port to the local console
- Output the log information to remote Telnet terminal or monitor, this function is good for remote maintenance
- Assign a proper log buffer zone inside the switch, for record the log information permanently or temporarily
- Configure the log host, the log system will directly send the log information to the log host, and save it in files to be viewed at any time

Among above log channels, users rarely use the console monitor, but will commonly choose the Telnet

terminal to monitor the system operation status. However information outputted from these channels are of low traffic capacity and can not be recorded for later view. The other two channels---the log buffer zone and log host channel are two important channels

SDRAM (Synchronous Dynamic Random Access Memory) and NVRAM (Non Vulnerable Random Access Memory) is provided inside the switch as two part of the log buffer zone, The two buffer zone record the log information in a circuit working pattern, namely when log information need to be recorded exceeds the buffer size, the oldest log information will be erased and replaced by the new log information, information saved in NVRAM will stay permanently while those in SDRAM will lost when the system restarts or encounter an power failure. Information in the log buffer zone is critical for monitoring the system operation and detecting abnormal states.



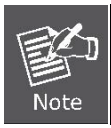
the NVRAM log buffer may not exist on some switches, which only have the SDRAM log buffer zone.
It is recommended to use the system log server. By configuring the log host on the switch, the log can be sent to the log server for future examination.

35.7.1.2 Format and Severity of the Log Information

The log information format is compatible with the BSD syslog protocol, so we can record and analyze the log by the systlog (system log protect session) on the UNIX/LINUX, as well as syslog similar applications on PC.

The log information is classified into eight classes by severity or emergency procedure. One level per value and the higher the emergency level the log information has, the smaller its value will be. For example, the level of critical is 2, and warning is 4, debugging is leveled at 7, so the critical is higher than warnings which no doubt is high than debugging. The rule applied in filtering the log information by severity level is that: only the log information with level equal to or higher than the threshold will be outputted. So when the severity threshold is set to debugging, all information will be outputted and if set to critical, only critical, alerts and emergencies will be outputted.

Follow table summarized the log information severity level and brief description.



these severity levels are in accordance with the standard UNIX/LINUX syslog.

Table 36-1 Severity of the log information

Severity	Value	Description
emergencies	0	System is unusable
alerts	1	Action must be taken immediately
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions
notifications	5	Normal but significant condition

informational	6	Informational messages
debugging	7	Debug-level messages

Right now the switch can generate information of following four levels

- Restart the switch, mission abnormal are classified critical
- Up/down interface, topology change, aggregate port state change of the interface are notifications warnings
- Outputted information from the CLI command is classified informational
- Information from the debugging of CLI command is classified debugging

Log information can be automatically sent to corresponding channels with regard to respective severity levels. Amongst the debugging information can only be sent to the monitor. Those with the Informational level can only be sent to current monitor terminal, such as the information from the Telnet terminal configuration command can only be transmitted to the Telnet terminal. Warnings information can be sent to all terminal with also saved in the SDRAM log buffer zone. And the critical information can be save both in SDRAM and the NVRAM (if exists) besides sent to all terminals. To check the log save in SDRAM and the NVRAM, we can use the show logging buffered command. To clear the log save in NVRAM and SDRAM log buffer zone, we can use the clear logging command.

35.7.2 System Log Configuration

System Log Configuration Task Sequence:

1. Display and clear log buffer zone
2. Configure the log host output channel

1. Display and clear log buffer zone

Command	Description
Admin Mode	
show logging buffered [level {critical | warnings} | range <*begin-index*> <*end-index*>]	Show detailed log information in the log buffer channel.
clear logging sdram	Clear log buffer zone information.

2. Configure the log host output channel

Command	Description
Global Mode	
logging {<*ipv4-addr*> | <*ipv6-addr*>} [facility <*local-number*>] [level <*severity*>] **no logging {<*ipv4-addr*> | <*ipv6-addr*>} [facility <*local-number*>]**	Enable the output channel of the log host. The “no” form of this command will disable the output at the output channel of the log host.

logging loghost sequence-number **no logging loghost sequence-number**	Add the loghost sequence-number for the log, the no command does not include the loghost sequence-number.

35.7.3 System Log Configuration Example

Example 1:

When managing VLAN the IPv4 address of the switch is 100.100.100.1, and the IPv4 address of the remote log server is 100.100.100.5. It is required to send the log information with a severity equal to or higher than warnings to this log server and save in the log record equipment local1.

Configuration procedure:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 100.100.100.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 100.100.100.5 facility local1 level warnings
```

Example 2:

When managing VLAN the IPv6 address of the switch is 3ffe:506::1, and the IPv4 address of the remote log server is 3ffe:506::4. It is required to send the log information with a severity equal to or higher than critical to this log server and save the log in the record equipment local7.

Configuration procedure

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 3ffe:506::1/64
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 3ffe:506::4 facility local7 level critical
```

Chapter 36 Reload Switch after Specified Time

36.1 Introduce to Reload Switch after Specifid Time

Reload switch after specified time is to reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully.

36.2 Reload Switch after Specifid Time Task List

1. Reload switch after specified time

Command	Explanation
Admin mode	
reload after *<HH:MM:SS>*	Reload the switch after a specified period of time.
reload cancel	Cancel the specified time period to reload the switch.

Chapter 37 Debugging and Diagnosis for Packets Received and Sent by CPU

37.1 Introduction to Debugging and Diagnosis for Packets Received and Sent by CPU

The following commands are used to debug and diagnose the packets received and sent by CPU, and are supposed to be used with the help of the technical support.

37.2 Debugging and Diagnosis for Packets Received and Sent by CPU Task List

Command	Explanation
Global Mode	
cpu-rx-ratelimit total <*packets*> **no cpu-rx-ratelimit total**	Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default.
cpu-rx-ratelimit queue-length <*queue-id*> <*qlen-value*> **no cpu-rx-ratelimit queue-length [<*queue-id*>]**	Set the length of the specified queue, the no command set the length to default.
cpu-rx-ratelimit protocol <*protocol-type*> <*packets*> **no cpu-rx-ratelimit protocol [<*protocol-type*>]**	Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default.
clear cpu-rx-stat protocol [<*protocol-type*>]	Clear the statistics of the CPU received packets of the protocol type.
cpu-rx-ratelimit channel <*channel-id*> <*packets*> **no cpu-rx-ratelimit channel [<*channel- id*>]**	This command is not supported by switch.
Admin Mode	
show cpu-rx protocol [<*protocol-type*>]	Show the information of the CPU received packets of the protocol type.
debug driver {receive|send} [interface {<*interface-name*> |all}] [protocol {<*protocol-type*> |discard |all}][detail]	Turn on the showing of the CPU receiving or sending packet informations.
no debug driver {receive |send}	Turn off the showing of the CPU receiving or sending packet informations.

Chapter 38 APPENDEX A

38.1 A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

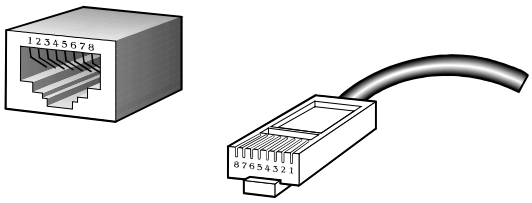
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

38.2 A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	**MDI** **Media Dependant** **Interface**	**MDI-X** **Media Dependant** **Interface-Cross**
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

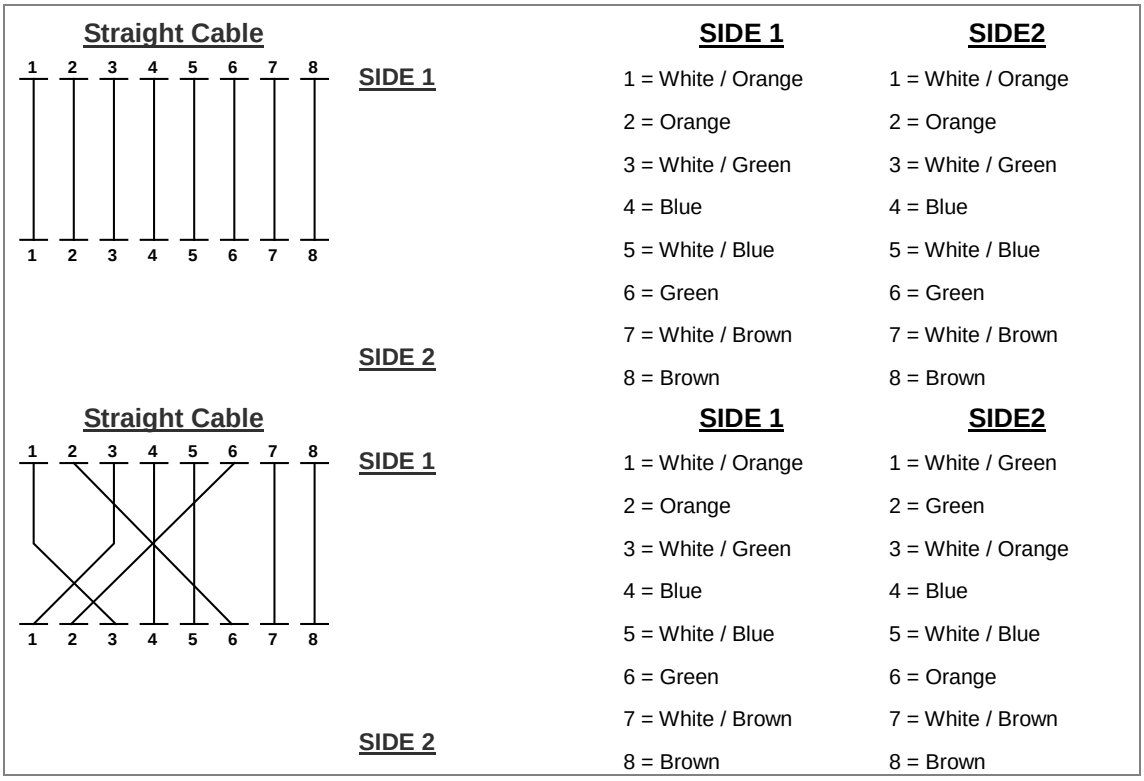


Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

Chapter 39 GLOSSARY

Bandwidth Utilization

The percentage of packets received over time as compared to overall bandwidth.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

Distance Vector Multicast Routing Protocol (DVMRP)

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Broadcasting (RPB).

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment such that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end-stations with multicast groups. GMRP requires that any participating network devices or end-stations comply with the IEEE 802.1p standard.

ICMP Router Discovery

ICMP Router Discovery message is an alternative router discovery method that uses a pair of ICMP messages on multicast links. It eliminates the need to manually configure router addresses and is independent of any specific routing protocol.

Internet Control Message Protocol (ICMP)

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is elected “querier” and assumes the responsibility of keeping track of group membership.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is directly related to the hardware interface for network devices and passes traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services no attached host has registered for, or forwards them to all ports contained within the designated multicast VLAN group.

Open Shortest Path First (OSPF)

OSPF is a link state routing protocol that functions better over a larger network such as the Internet, as opposed to distance vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobtrusively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Routing Information Protocol (RIP)

The RIP protocol attempts to find the shortest route to another device by minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Simple Network Management Protocol (SNMP)

The application protocol offering network management services in the Internet suite of protocols.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol, a standard protocol for point-to-point connections using serial lines.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or back-up linked network systems. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

EC Declaration of Conformity

For the following equipment:

*Type of Product: 50-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
*Model Number: WGSW-50040

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 11F, No 96, Min Chuan Road,
Hsin Tien, Taipei, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(1998 + A1:2000 + A2:2003, Class A)
EN 61000-3-2	(2000 + A2:2005 Class D)
EN 61000-3-3	(1955 + A1:2001 + A2:2005)
EN 55024	(1998 + A1:2001 + A2:2003)
IEC 61000-4-2	(1995 + A1:1998 + A2:2000)
IEC 61000-4-3	(2002 + A1:2002)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(1995 + A1:2000)
IEC 61000-4-6	(1996 + A1:2000)
IEC 61000-4-8	(1993 + A1:2000)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**1th Sep, 2010**	Kent Kang
Place	*Date*	*Legal Signature*